

**user's
guide**

hp surestore nas 8000

user's guide



Edition March 2002
Part number A7418-96001



Notice

© Hewlett-Packard Company, 2002. All rights reserved.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice.

Format Conventions

WARNING Identifies a hazard that can cause personal injury

Caution Identifies a hazard that can cause hardware or software damage

Note Identifies significant concepts or operating instructions

Computer font — used for all text to be typed verbatim: all commands, path names, file names, and directory names also, text displayed on the screen

Italics font — used for variables used in commands

Bold font — used for screen menu options and controls

Trademark Information

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Microsoft, Windows, and Windows NT are U.S. registered trademarks of Microsoft Corporation.

UNIX is a registered trademark of The Open Group.

1 HP NAS 8000 Overview 9

What is NAS? 9

Product Overview 10

Hardware 10

Software 12

Product Configurations 13

Direct-Attached Configuration 13

Direct-Attached Configuration with High Availability 14

SAN Configuration 17

SAN Configuration with High Availability 18

User's Guide Overview 19

2 NAS 8000 Concepts 21

Understanding Physical and Logical Storage 21

Physical Storage 22

Disk Drives 22

Logical Storage 23

Logical Unit Number 23

Volume Groups 23

File Volumes 23

Directories 23

Snapshots 23

Understanding High Availability 24

Cluster Components 24

Failover Models 25

Active/Active Failover Model 26

Active/Passive Failover Model 26

Resource Model 26

Failover Packages	27
Eliminating Single Points of Failure	27
High-Availability Options in the Command View NAS Web Interface	28
About HP NAS Server Security	29
HP NAS Server Security in a UNIX-only Environment	29
HP NAS Server Security in an NT-only Environment	30
Share-Level Security	31
User Level (Domain) Security	31
Permissions	32
Sharing Files Across Multiple Platforms	32
Accessing Files Created by UNIX Clients	33
Accessing Files Created by NT Clients	34

3 Getting Started 35

Using the Command View NAS Web Interface	35
Downloading the Sun Microsystems Java™ Plug-In	38
Using Online Help	39
Printing Help Information	39
Task Overview	40
Prerequisites	40
Management Tasks	40

4 Configuring Your System and Network 43

Using the Configuration Wizard	44
Identifying your NAS Server	46
Shutting Down and Restarting	47
Direct-Attached and SAN Configuration	47
High-Availability Configuration	48
Configuring System Security	49
Editing the Command View NAS Access List	49
Setting an Administrative Password	49
Configuring System Settings	51
Defining the System Name	51
Setting the Date and Time	52
Assigning Contact Information	52

Configuring TCP/IP Settings	54
Defining IP Addresses	54
Defining the Command View Management Port	56
Enabling Bonding	56
Setting the Domain Name Service (DNS)	58
Configuring High-Availability Settings	59
Cluster Configuration Overview	59
Entering Node Settings	61
Defining the Cluster Name	62
Defining the Quorum Server	62
Setting Timeouts and Intervals	63
Starting and Stopping Clustering Services	64
Configuring Networking Settings	66
Windows Settings	66
Specifying WINS Properties	66
Defining Windows Security	66
UNIX Settings	68
Specifying NIS Properties	68
Specifying NFS Properties	69
Configuring Alert Settings	70
Defining SNMP Alerts	70
Defining Email Alerts (SMTP)	71
Setting Up the Remote System Log	72
Configuring User and Group Mapping	73
Understanding User and Group Mapping	73
Importing and Exporting Users or Groups	75
Configuring UPS Connections	76

5 Managing Your Storage 77

Managing Arrays and LUNs	78
Viewing the Storage Array Summary	78
Scanning for New Storage	79
Renaming an Array	79
Using Advanced Array Management	80
Creating a LUN	80
Deleting a LUN	81

Managing Volume Groups	82
Viewing Volume Groups	82
Creating a Volume Group	82
Editing a Volume Group	83
Deleting a Volume Group	84
Managing Failover Packages	85
Viewing Failover Packages	85
Adding a New Package	86
Editing a Package	87
Deleting a Package	88
Starting a Package	88
Stopping a Package	89
Failing Over a Package	89
Failing Back a Package	90
Managing File Volumes	91
Viewing File Volume Information	91
Creating a New File Volume	92
Editing a File Volume	93
Deleting a File Volume	94
Managing Shares and Exports	95
Viewing Shares and Exports	95
Creating or Editing an SMB Share	96
Creating or Editing an NFS Export	97
Deleting a Share or Export	97
Verifying that the HP NAS Server Is Accessible to Users	98
Creating a Directory	98
Renaming a Directory	99
Deleting a Directory	99
Replicating Data with Snapshots	100
Using Snapshots	100
Creating a Snapshot	101
Editing a Snapshot	102
Deleting a Snapshot	102
Scheduling a Snapshot	103
Managing Quotas	105
Understanding Quotas	105

Enabling or Disabling Quotas	105
Managing User Quotas	106
Configuring User Quotas	106
Adding a User Quota	107
Editing a User Quota	107
Deleting a User Quota	108
Importing and Exporting User Quotas	108
Managing Group Quotas	109
Configuring Group Quotas	109
Adding a Group Quota	110
Editing a Group Quota	110
Deleting a Group Quota	111
Importing and Exporting Group Quotas	111

6 Monitoring the System 113

Viewing the Status Summary	115
Storage Array Status	116
Environment	116
Performance	116
Monitoring the NAS Server	117
Monitoring Events	117
Viewing the Hardware Event Log	117
Viewing the System Log	118
Monitoring the Environment	119
Viewing Temperature Status	119
Viewing System Voltage Status	119
Viewing Cooling Fan Status	120
Monitoring Components	121
Viewing Memory Status	121
Viewing Power Supply Status	121
Viewing UPS Status	122
Monitoring Performance	123
Viewing CPU Utilization	123
Viewing Network Activity	123
Viewing Client Activity	124
Monitoring High-Availability Settings	125
Monitoring Nodes	125

Monitoring Failover Packages 125

7 Enabling Virus and Backup Software 127

Using NAS Virus Protection 128

Overview 128

Updating the Virus File 130

Using Scheduled Scan Control 131

Understanding Scheduled Scan Control 131

Creating and Editing a Scan Task 131

Performing a Scan Task and Viewing the Status 133

Copying a Scan Task 134

Deleting a Scan Task 134

Using Real Time Protection Control 135

Understanding Real Time Protection Control 135

Creating and Editing an RTP Task 135

Changing RTP Global Settings 136

Deleting an RTP Task 137

Managing Quarantined Files 137

Viewing Virus Logs 139

Using the Backup Agent 140

Connecting Tape Devices 141

Using HP OpenView OmniBack II and the NAS Backup Agent 141

Enabling the NAS 8000 Backup Agent 142

Importing the Client to an OmniBack II Cell 143

Configuring a Backup Device 144

Configuring the Tape Drives 144

Backing Up Files 145

Managing and Configuring the HP OpenView OmniBack II NAS Agent 147

Snapshot Behavior: Per-volume Snapshot Backup 148

Troubleshooting the OmniBack Agent 149

Enabling Snapshots 152

8 Recovering from a Disaster 153

Restoring the NAS Server Configuration 154

Restoring Storage Array Settings 155

Restoring the NAS Server and Storage Array 157

9 Integrating with Network Backup Applications 159

- Using HP OpenView OmniBack II 161
 - OmniBack II User Interface for Windows NT 162
 - OmniBack II User Interface for UNIX 164
- Using Computer Associates ARCserve 2000 165
 - ARCserve 2000 for Windows NT 165
- Using Veritas Backup Exec 167
- Using Veritas NetBackup 169
 - NetBackup for Windows 169
 - NetBackup for UNIX 170
- Using IBM Tivoli Storage Manager 171
 - Storage Manager for Windows 171
 - Storage Manager for UNIX 172
- Using Legato NetWorker 173
 - Networker for Windows 173
 - Networker for UNIX 174

10 Obtaining Product Support and Software Upgrades 175

- Contacting HP NAS Server Service and Support 176
 - HP NAS Server Support Web Site 176
 - Contact Customer Support 176
- Viewing the Command View NAS License 177
- Viewing Open Source Code 178
- Using Array Diagnostics 179
- Upgrades 180
 - Upgrading NAS Server Software 180
 - Upgrading Storage Array Firmware 181

A NAS 8000 System and Hardware Upgrades 183

- System Upgrades 183
 - Upgrading to a High-Availability System 183
- Hardware Upgrades and Replacements 184
 - NAS Server Upgrades 184

Adding NICs	184
Assigning IP Addresses	186
Firmware Upgrades	186
Standard Server Upgrades	186
Storage Array Upgrades	187
Adding Disks	187
Modifying Storage Settings	187
Tape Library Upgrade	190
Adding a Tape Library	190
Installing SCSI or FC HBA Cards	190
Firmware Upgrades	194
UPS Upgrade	195
Adding a UPS	195
UPS Product Information	196

B SNMP Trap Definitions 197

C Legal Information 201

Acknowledgments	201
HP Surestore Software License Agreement	203
Safety and Regulatory Information	208
HP NAS Server Warranty Information	209
Warranty Information	209
Hewlett-Packard Limited Warranty Statement	211

D Command View SDM Limitations 213

E Command View NAS Command Line Interface 221

F Glossary 223

HP NAS 8000 Overview

1

What is NAS?

Network-attached storage (NAS) is a storage solution attached to a network that is optimized for file sharing and serving. NAS provides a simple, reliable, and cost-effective way to add storage to networks. Because a NAS device is designed specifically for storage, it requires minimal setup and is easily maintained. NAS devices also have built-in redundancy features to protect against failure and downtime.

A NAS solution typically consists of a server, a set of disk drives, a custom operating system, and a built-in web interface for managing storage. NAS devices provide file services to a mixture of clients that operate in a heterogeneous network environment. A NAS device can be added to an existing LAN network to increase storage capacity.

How is NAS different from SAN (Storage Area Network)? In many respects they are similar and can use the same hardware, but the SAN requires its own high-speed storage network, while the NAS lives on an already existing LAN. A NAS device is designed to move files, whereas the SAN is designed to provide block-level data at high speeds to application servers. SAN solutions are typically more difficult to implement and more expensive than NAS solutions.

Product Overview

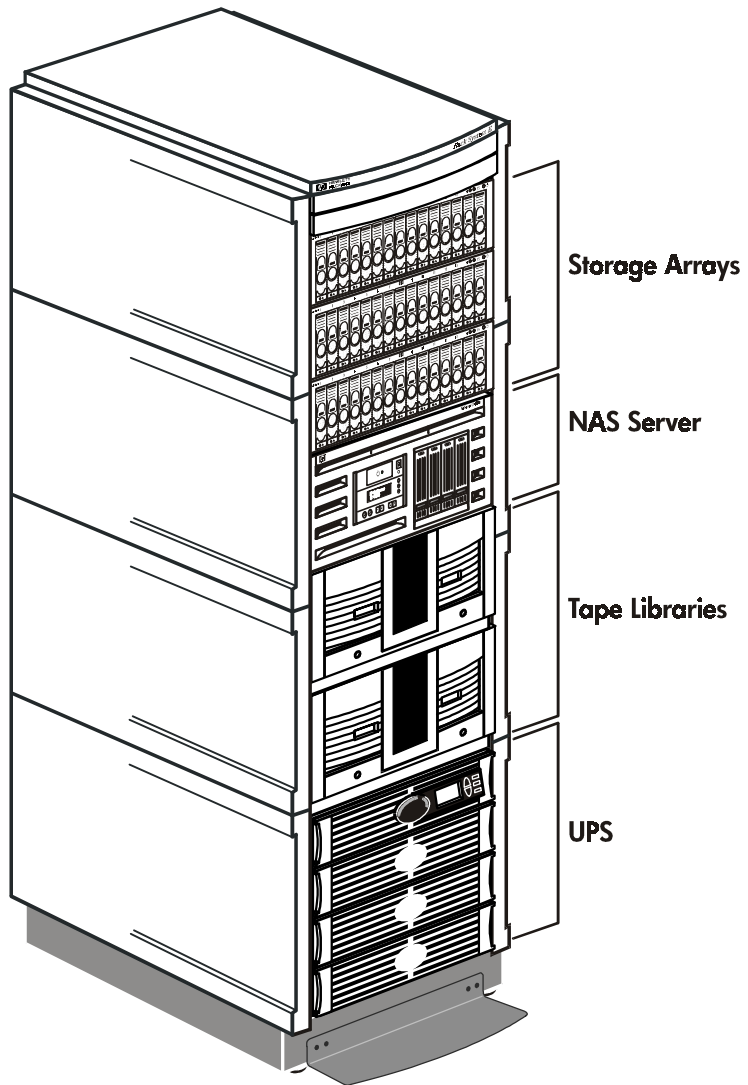
The HP Surestore Network-Attached Storage (NAS) 8000 series offers several storage solutions that attach directly to your network and provide shared file storage for workgroups and departments.

Hardware

The NAS 8000 solution can include one or more of the following, sold separately or pre-installed in a rack:

- A NAS server with a custom operating system.
 - Network interface cards (NICs). The server comes with one 10/100TX port, and you can add up to two dual-port 10/100TX NICs or two single-port gigabit NICs.
- Storage arrays:
 - Direct-attached to the NAS server. The HP Virtual Array (VA) 7100 and 7400 series can have up to 15 drives (18, 36 and 73 GB capacity); the VA7400 series supports up to six JBODs attached to each array for additional storage capacity.
 - Remotely connected via a SAN network. HP VA and XP arrays are supported.
- Fiber channel switches for multiple array configurations.
- Quorum server with cluster management software for high-availability solutions.

Figure 1 NAS Racked System



Other accessories sold separately are:

- Uninterruptible power supply (UPS).
- HP Surestore tape libraries.

Software

The NAS 8000 server comes preloaded with:

- A custom operating system optimized for file serving. A command line interface is available for advanced server management.
- HP Command View NAS management software that runs in a web browser. This graphical user interface is the primary tool for managing the NAS 8000. Links to Command View SDM are provided for advanced array management.
- HP Virus Guard virus protection software, which is integrated with the NAS operating system and Command View NAS.
- A server backup agent for HP OmniBack II 4.1, which is integrated with the NAS operating system and Command View NAS.
- File volume snapshot capability for data protection.

If you do not use the NAS 8000 backup agent, you can backup your data using one of the following network backup software products:

- HP OmniBack II
- Computer Associates ARCserve 2000
- Veritas Backup Exec
- Veritas NetBackup
- IBM Tivoli Storage Manager
- Legato Networker

You can also integrate the NAS 8000 with several network management software products, including HP OpenView Network Node Manager. For more information about network management plug-ins, see <http://www.hp.com/support/emsp> to learn about the HP Surestore Enterprise Integrations product.

Additional NAS 8000 integrations with other products, such as Oracle and SQL server may be possible. See <http://www.hp.com/support/nas8000> for a current description of supported product integrations.

Product Configurations

The NAS 8000 is available in four configurations:

- Direct-attached storage configuration
- Direct-attached storage configuration with high availability
- SAN configuration
- SAN configuration with high availability

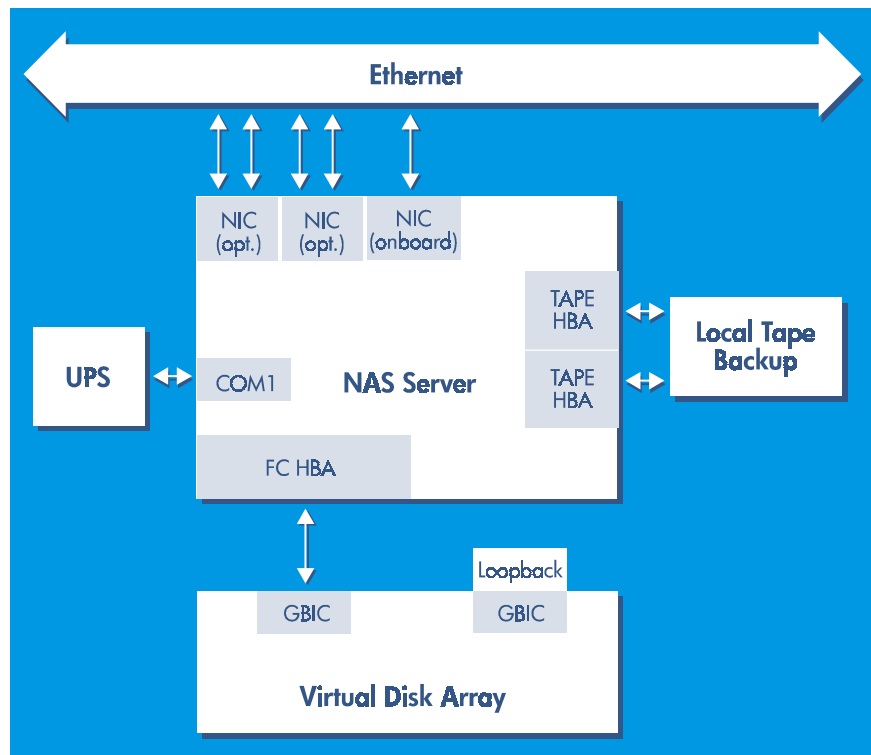
Depending on the configuration of your NAS server, different options display in the Command View NAS web interface.

Direct-Attached Configuration

With direct-attach configurations, one HP VA7100 or VA7400 series disk array is connected to the NAS server using one Fibre Channel (FC) Host Bus Adapter (HBA). In addition:

- The server includes one internal NIC with the option of adding two additional NICs.
- The server may include two SCSI or FC HBAs for connecting to an optional tape library.
- The server communicates with an optional UPS using a serial connection.

Figure 2 Direct Attached Configuration

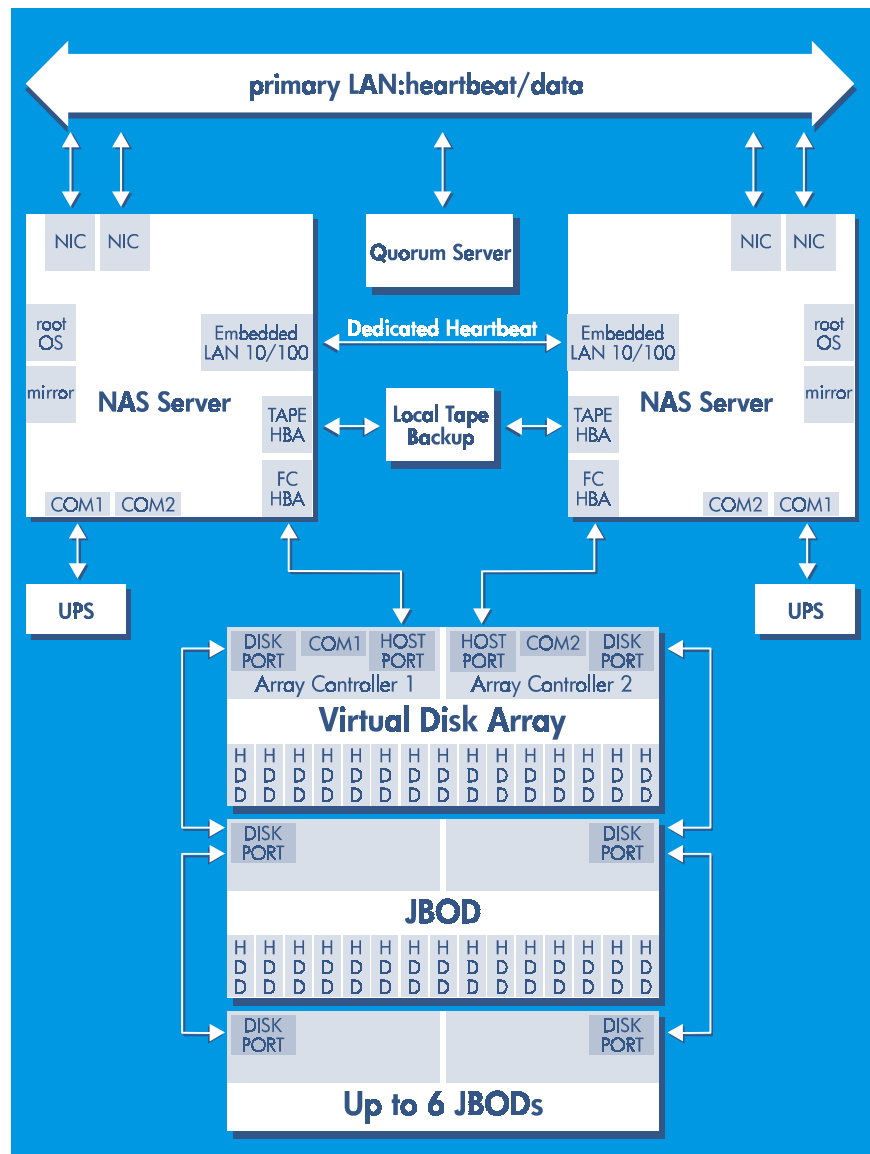


Direct-Attached Configuration with High Availability

In direct-attached configurations with high availability, one or two VA7100 or VA7400 series disk arrays are attached to a cluster consisting of two NAS servers and a Quorum server that manages the high-availability services for the cluster. In addition:

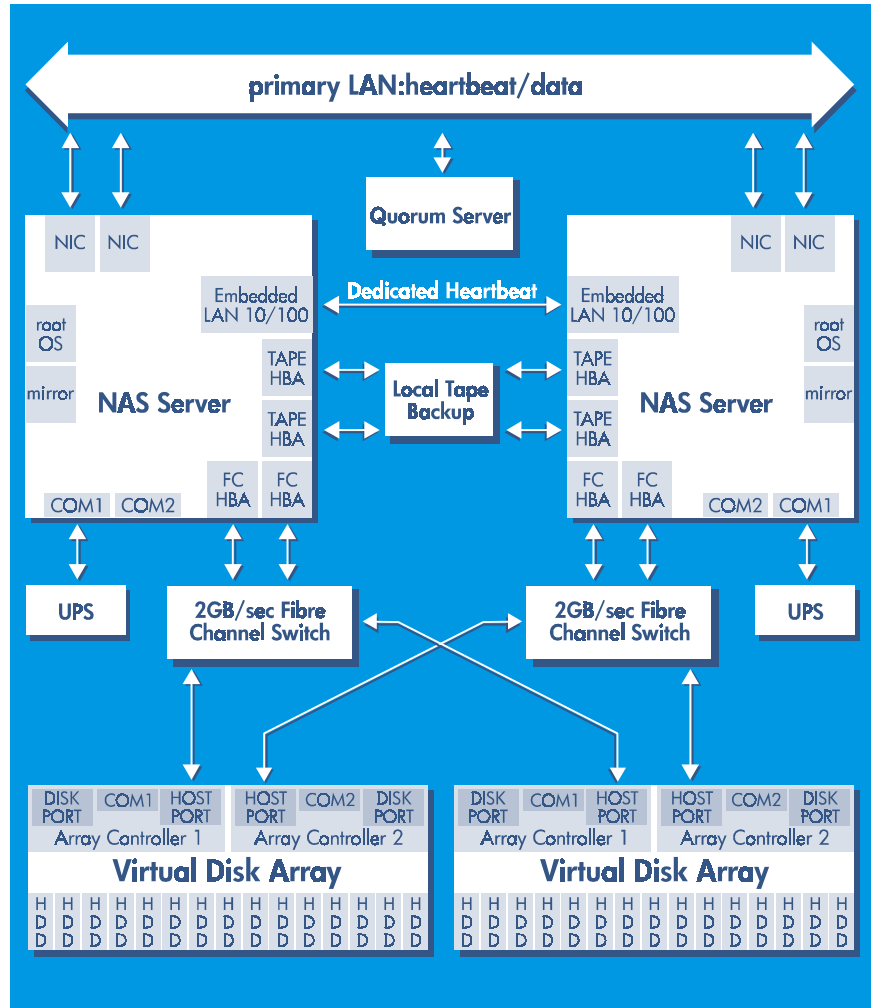
- A single HBA is pre-installed in each server.
- A separate UPS is required for each NAS server.
- Tape backup can be shared by both NAS servers.

Figure 3 Direct-Attached Configuration with High Availability



- Multiple arrays may also be attached using FC switches.

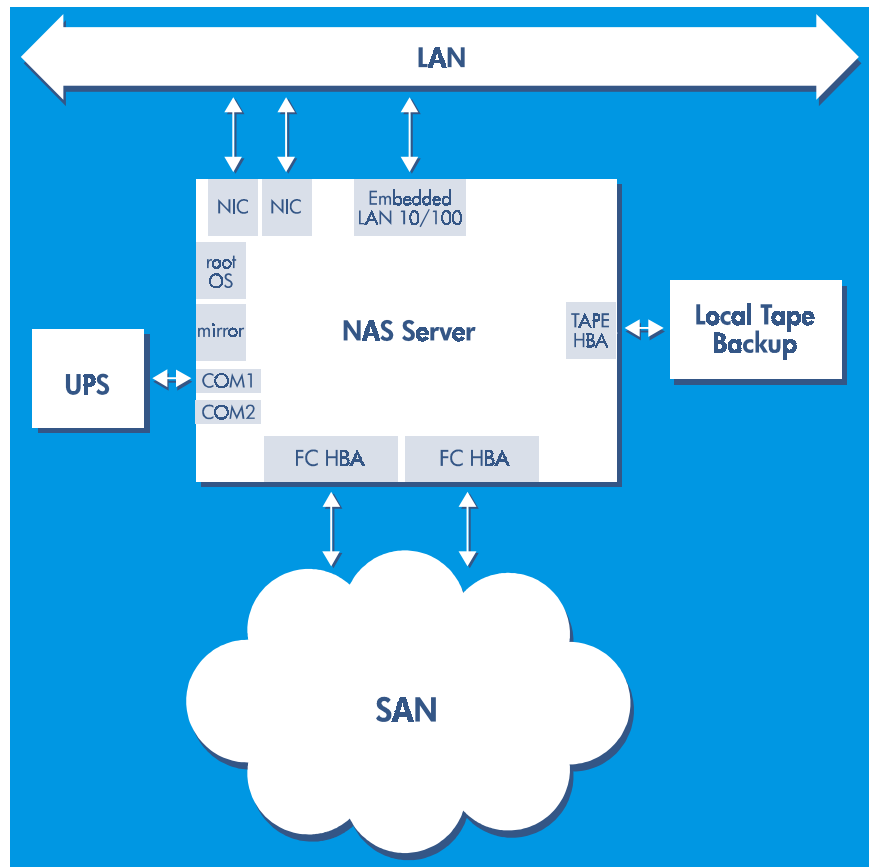
Figure 4 Multiple Arrays with FC Switches



SAN Configuration

NAS 8000 solutions can also manage storage on HP VA7100, VA7400 series or XP model arrays connected to a SAN. LUNs must be created and assigned to the NAS 8000 using a product such as HP Surestore Secure Manager VA or Secure Manager XP.

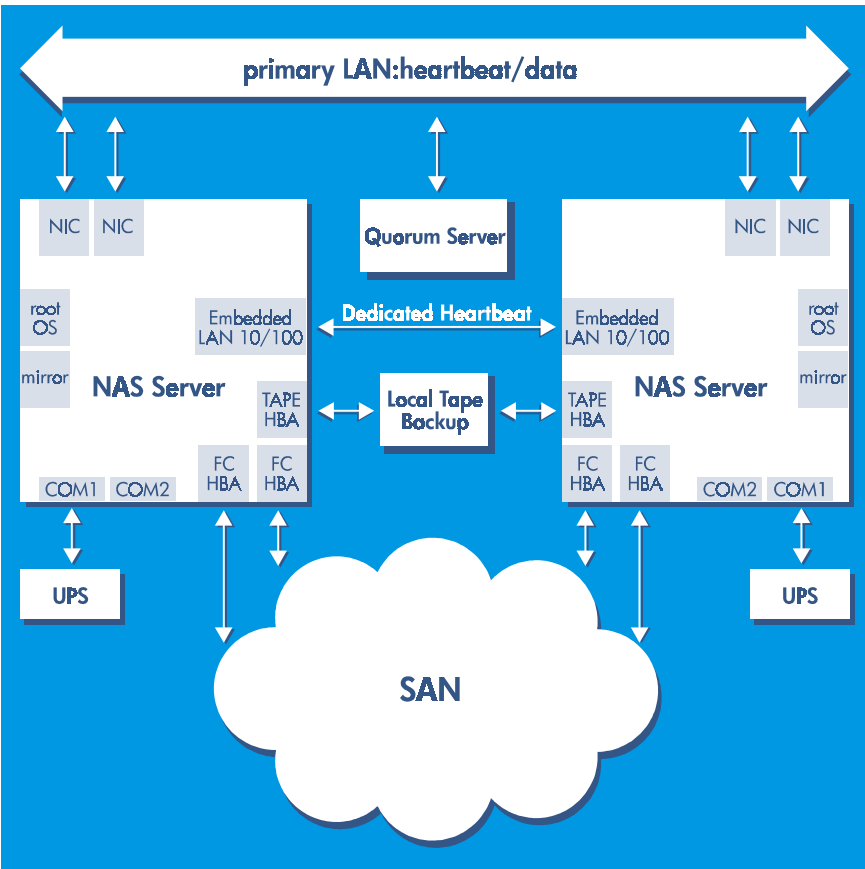
Figure 5 SAN Configuration



SAN Configuration with High Availability

A high-availability, clustered NAS 8000 system can also be configured to access VA7100, VA7400 series and XP model arrays attached via SAN.

Figure 6 SAN Configuration with High Availability



User's Guide Overview

This user's guide is organized into the following chapters:

Chapter	Description
Chapter 1, HP NAS 8000 Overview	Introduction to the features of the HP NAS 8000.
Chapter 2, NAS 8000 Concepts	Key concepts you need to know about storage and security.
Chapter 3, Getting Started	What you need to do to begin using the HP NAS 8000.
Chapter 4, Configuring Your System and Network	Set up your system, TCP/IP, networking, and alerts settings. If you have a high-availability NAS server, enter those settings here. You can also configure user and group mapping, and monitor UPS connections.
Chapter 5, Managing Your Storage	Set up LUNs, volume groups, failover packages (if you have a high-availability system), file volumes, shares, exports, snapshots, and quotas.
Chapter 6, Monitoring the System	Monitor the NAS server's events, environment, components, and performance. You can also monitor high-availability settings and any attached arrays.
Chapter 7, Enabling Virus and Backup Software	Use virus-protection software, backup agent, and snapshots to protect your data.
Chapter 8, Recovering from a Disaster	Restore your storage system to its originally configured state.
Chapter 9, Integrating with Network Backup Applications	Use network backup applications with your NAS server.
Chapter 10, Obtaining Product Support and Software Upgrades	Contact support, view Open Source code, run diagnostic tools, and obtain software upgrades.
Appendices	Obtain system and hardware upgrades, trap definitions, legal information, Command View SDM overview, and the Command View NAS Command Line Interface.

NAS 8000 Concepts

2

Understanding Physical and Logical Storage

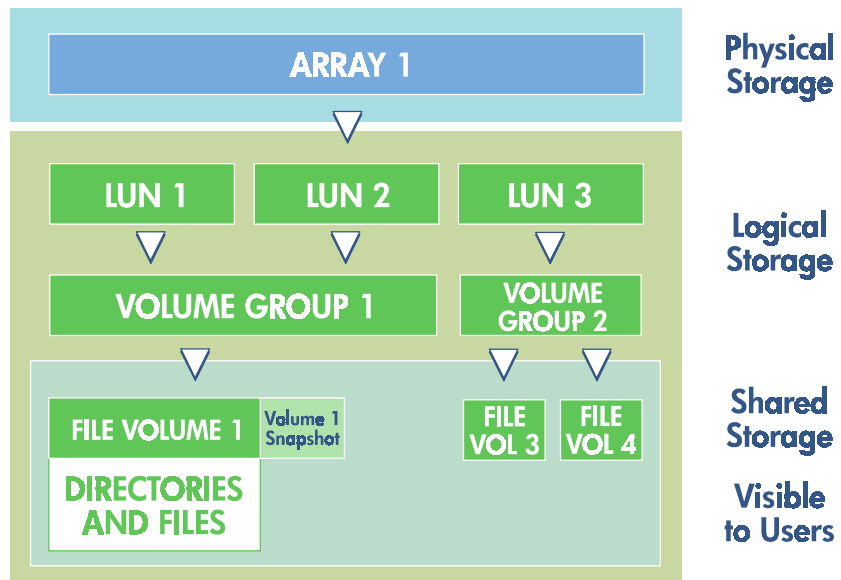
The storage space on your HP NAS 8000 is made up of physical storage and logical storage for a direct-attached and SAN configuration. Before you begin planning your storage, you need to understand the following concepts.

Physical storage refers to the hardware used for data storage. The physical storage components of the HP NAS 8000 are the disk drives.

Logical storage is created by software that lets you combine disk space from multiple physical disks into a logical volume. The logical storage components of the HP NAS 8000 include:

- Logical unit numbers (LUNs)
- Volume groups
- File volumes
- Directories
- Snapshots

Figure 1 Physical and Logical Storage



Physical Storage

Disk Drives

The HP NAS 8000 supports the following storage devices either directly attached to the NAS 8000 or on a SAN:

- Virtual Array (VA) 7100 is a disk storage system that holds from 4 to 15 disk drives. The array has scalable capacities from 72 GB to over 1 Terabyte depending upon the size and number of disk drives. The capacity of the disk drives can be mixed.
- Virtual Array 7400 series arrays are high-performance, high-availability, multi-terabyte storage arrays with a 2Gb/s fibre channel host. The VA7400 series supports up to 105 drives (10 minimum) with additional DS2400 disk enclosures.

For more information about these drives, see the *HP Surestore Virtual Array VA7100 and VA7400 User And Service Guides* at <http://www.hp.com/support/va7100> or <http://www.hp.com/support/va7400>.

Logical Storage

The HP NAS 8000 lets you set up your storage into these logical divisions:

Logical Unit Number

A logical unit number (LUN) is a logical aggregation of the space on one or more physical drives. The HP NAS 8000 supports a maximum of 127 LUNs.

Volume Groups

A volume group is the aggregation of one or more LUNs. Volume groups combine the space from LUNs and make the space accessible to the file system for creating file volumes and directories, which can then be made accessible to users.

File Volumes

A volume group is divided into one or more file volumes. File volumes are the basic unit of logical storage for a file system on the HP NAS 8000. File volumes can be further subdivided into individual directories.

Directories

Directories let you organize information. Directories contain files or other persistent data structures in a file system that contains information about other files. Directories are usually organized hierarchically and may contain both files and other directories, and are used to organize collections of files for applications or convenience.

Snapshots

A snapshot is a read-only picture of a file volume at a specific point in time that provides almost instantaneous access to the previous snapshot version of a file.

Understanding High Availability

Note

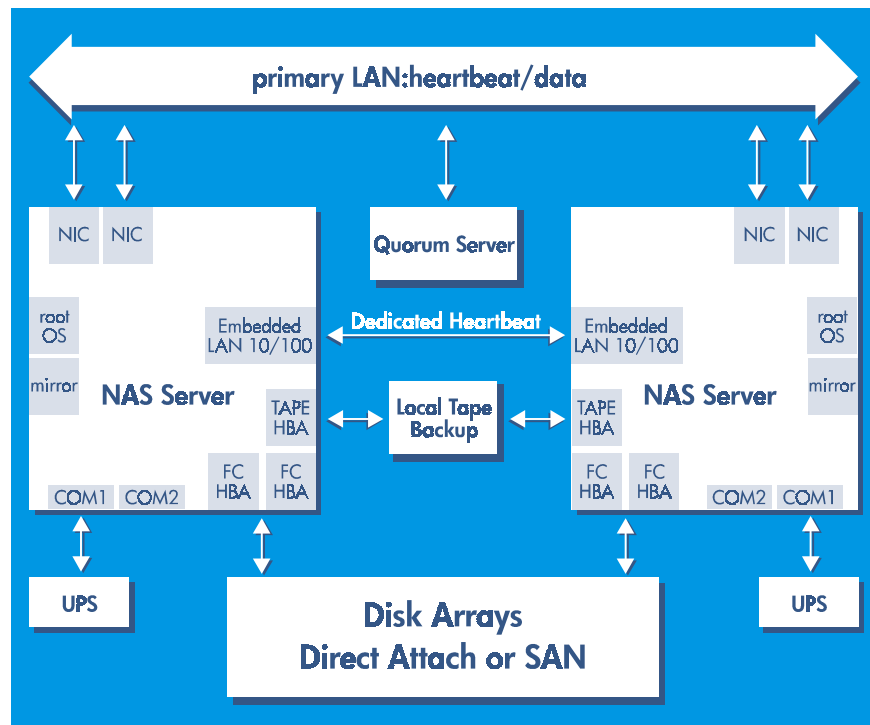
This section applies only if you have purchased a high-availability NAS solution.

High availability characterizes a system that is designed to avoid the loss of service by reducing or managing failures and minimizing downtime. High availability implies a service level in which both planned and unplanned downtime is minimized.

Cluster Components

The HP NAS 8000 cluster consists of two NAS servers, a Quorum server and storage that may come from either a direct-attached configuration or a SAN. The NAS servers share access to the storage and provide failover capabilities for each other, but function as independent servers. The main purpose of high-availability clusters is to provide a higher degree of storage availability to client systems than is possible with a single server. This is accomplished by minimizing single points of failure and providing functional redundancy. Server downtime and interruptions to storage availability are minimized by failing over file serving capabilities between the NAS servers in the event of a failure in either server.

Figure 2 Cluster Components



Failover Models

Failover is a backup operational mode in which the functions of one NAS server are assumed by the other NAS server when a NAS server becomes unavailable through failure or scheduled down time.

The following two modes are supported for the NAS servers in the cluster:

- Active/Active
- Active/Passive

Active/Active Failover Model

In the active/active failover model, both NAS servers provide simultaneous access to storage. Each NAS server maintains separate file systems, CIFS shares, and NFS exports. The NAS servers do not provide shared access to the same volumes and file systems simultaneously. Each NAS server functions as a separate file server. To facilitate file system failover, the NAS servers have full access to each other's disk resources but do not utilize the shared access unless a server failure occurs. When the failure criteria have been met and the failover system directs a NAS server to fail over, the NAS server then takes over the IP and disk resources of the failed server and begins serving the file systems and associated shares as if they were its own. Note that both NAS servers provide CIFS and NFS services.

Active/Passive Failover Model

In the active/passive failover model, only one NAS server is active at a time. The other NAS server waits in standby mode until a failover occurs. The active NAS server operates as in the active/active model, providing both CIFS and NFS services to client systems. Active/passive mode is created by starting failover packages on only one primary server and configuring the secondary server to be the failover target in the event of a primary server failure.

Resource Model

The cluster has a shared-nothing resource model, which means that each server has exclusive access to the storage (volume groups, volumes, and shares) and network resources (hostname, package names, IP addresses) that it's serving. The cluster nodes can see each others' storage and are aware of each others' packages and IP addresses, but by agreement and design, they activate only the storage and network addresses to which they are currently assigned. The clustering system strictly enforces this agreement to prevent concurrent or shared access to the same storage resources. The file system that is used for each file volume is not distributed and does not support simultaneous shared access. The cluster Quorum server's primary job is to enforce the shared-nothing cluster policy.

Failover Packages

Failover packages are the smallest unit of failover within the cluster. A package contains necessary definitions and configuration information relating to resources and their processes that must be failed over to the secondary server in the event the primary server fails. Each cluster can have a maximum of 30 packages running concurrently. For NAS, the package defines the volumes (file systems) and their associated CIFS shares and NFS exports that should be failed over. A given volume group can be defined in only one package at a time, but a package can contain multiple volume group definitions. The packages can fail over automatically when a server fails, or they can be manually failed over one at a time. A given package can be running on only one cluster node at a time.

Think of a package as a group of one or more volume groups (with their file systems and shares/exports) that will fail over as a single unit. To fail over a package manually, you need to:

- Stop the existing package (in the case of a service, network, or resource failure).
- Start the new instance of the package on a different node.

You can manage failover packages on the Storage tab of the Command View NAS web interface.

Eliminating Single Points of Failure

Most problems that result in service outages are single-level failures. High-availability lets you quickly detect and handle these failures and minimize downtime. Examples of single-level failures include:

- NIC failures
- NFS failure
- SMB failure
- Operating system failure
- Power failure

High-Availability Options in the Command View NAS Web Interface

You can manage high-availability options on the following tabs of the Command View NAS web interface:

- **Configuration tab:** Start or stop clustering services; manage node settings for your cluster; name your cluster; enter a name for the Quorum server; and set up timeouts and intervals for the cluster.
- **Storage tab:** Add, edit, delete, start, and stop failover packages. You can also manually fail over or fail back a package.
- **Status tab:** Monitor nodes and failover packages.

About HP NAS Server Security

Two basic ways to ensure the security of the NAS server are:

- Control access to the device
- Set an administrative password to ensure that only authorized users gain access to key administrative functions

Access and rights to the data that clients store on the NAS server can involve security in the Windows® and UNIX® environments. This section discusses key security elements that you might consider when administering your NAS server.

HP NAS Server Security in a UNIX-only Environment

UNIX uses a reasonably simple approach to data access security. Each workstation performs user authentication locally. Each user is associated with a 16-bit integer (user ID or UID). Additionally, each user can be a part of a group that is denoted by another 16-bit integer (group ID or GID). A user can be a member of several groups, each with its own unique GID. All objects contain associated meta-data that includes the UID and GID as well as read/write/execute permissions for the object. A typical UNIX file permission might look like:

```
-rwxr-xr-x 1 201 5 611 Nov 11 11:09 testfile
-rwxr-xr-x 1 Wilson Engineering 611 Nov 11 11:09
testfile
```

In the first line, numbers represent the UID and GID; in the second line, the names associated with the UID and GID are displayed. In either case, Wilson (UID 201), who is a member of the Engineering group (GID 5), created a file that has permissions for three different groups. The permissions are represented by a string of nine characters: three characters for the permissions of each of the three groups of users. The three groups are the owner (Wilson), the group (Engineering), and other. In the example above, the owner has specified `rwx` (read/write/execute) privileges for himself, `r-x` (read/execute) privileges for the group, and `r-x` (read/execute) privileges for other.

In your network, you might use a Network Information Service (NIS) server to help you maintain common configuration files such as the password, group, and host files. If your environment uses a NIS server, you can enable NIS. The

NAS server then maintains the same UID and GID numbers that your UNIX users are currently assigned in a heterogeneous environment.

Note Whether you disable or enable the use of a NIS server, you are in no way affecting the security of a homogenous UNIX environment.

An additional form of security called host access is available in the UNIX environment and controls which client machines are allowed access to the NAS server, regardless of the user. The allowed clients are specified by a list of IP addresses or hostnames representing those machines. Host access controls access by machine, not user.

HP NAS Server Security in an NT-only Environment

The security schema for NT systems is different from that of UNIX, but there are two similarities:

- You can set up the security model to allow user authentication at the share level; alternatively, you use a security domain, in which authentication is handled by a Primary Domain Controller (PDC) or Backup Domain Controller (BDC).
- Processes are run with an identity of a user and any groups to which that user belongs for either that workstation or the domain. Each data object is associated with meta-data, sometimes called a security descriptor (SD). The security descriptor contains a list of permissions or denials in the Access Control List (ACL), which contains an almost limitless number of permutations that can be associated with a data object.

The NAS server lets you choose between two security models:

- Share-level security
- User-level (Domain) security

Additionally, host access is available in the NT environment to control which client machines are allowed access to the NAS server, regardless of the user. The allowed clients are specified by a list of IP addresses or hostnames representing those machines. Host access controls access by machine, not user.

Share-Level Security

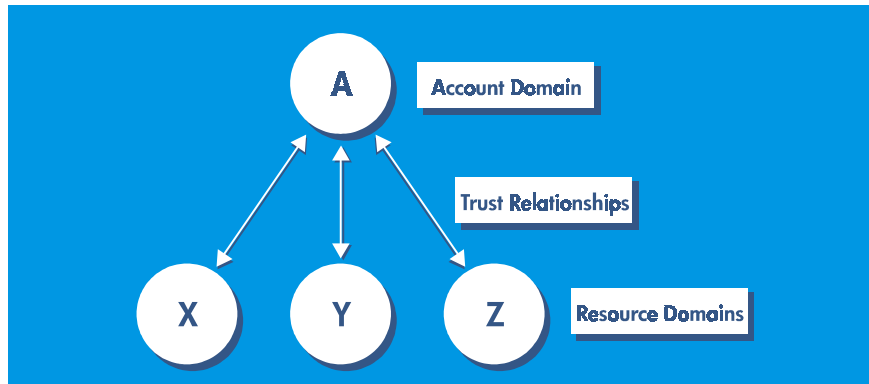
With share-level security, the server explicitly asks for permission (password) every time a user connects to a share on the NAS server. Thus, any user on the network who knows the name of the NAS server, the name of the resource (or file), and the password has access to the resource. When you are using share-level security, you can assign shares a read-only password and/or a read-write password.

User Level (Domain) Security

With user-level security, the client accessing the NAS server passes the credentials of the logged-on user to the NAS server system transparently. The NAS server in turn queries the Primary Domain Controller (PDC) or Backup Domain Controller (BDC) to authenticate the user. Once the user is authenticated, the PDC or BDC returns a Security ID (SID) that the NAS server uses to check the client's access rights. This token is then used with all subsequent requests from that client.

The NAS server supports the NT Master Domain model. This allows the NAS server to participate in a resource domain that is separate from the domain in which users are authenticated.

Figure 3 NT Master Domain Model



At boot-up time, the NAS server locates the PDC in the specified account domain, as well as the domain controller in the specified resource domain, then logs on to that domain.

Permissions

You can assign the following permissions to an NT resource:

- Read
- Delete
- Write
- Execute
- Change Permissions
- Take Ownership

Additionally, you can group these permissions into standard permissions that consist of one or more previous permissions. These standard permissions include:

- No Access
- Read
- Change
- Full Control
- Special Access (where individual permissions can be selected, such as Read + Change Permissions)

Sharing Files Across Multiple Platforms

The NAS server was designed to work well in a heterogeneous environment and support remote file access protocols for UNIX and NT clients. A major difficulty in sharing data across these environments is that the file system security models are very different. For example, NT systems that use user-level security use ACLs to identify both themselves and the permissions for each data object, whereas UNIX systems use traditional UNIX permissions that define explicit permissions for the user, group, and other. However, given some care in setting up the security environment, a reasonable level of access can be provided for cross-environment requests (i.e., a UNIX client requesting a file created by an NT client) without overly compromising the security set by the creator of the object.

Accessing Files Created by UNIX Clients

When an NT user accesses a UNIX file, the UNIX file permissions are translated into an ACL that then determines the permissions to grant. Recall from HP NAS Server Security in a UNIX-only Environment that permissions are granted to three distinct groups:

- user
- group
- other

If the owner of the UNIX file does not map to a user in the NT domain, then an NT user ID will be generated in the local UNIX domain. If the owner of the UNIX file is recognized (or mapped) as a known NT user, then the appropriate information will be exchanged so that the owner has the same security privileges in NT that he or she had in UNIX. A similar process occurs for the group identification and permissions. The **Other** field is mapped to the NT **Everyone** account.

This table shows the mapping that takes place between the permissions.

UNIX	NT Equivalent
r--	Read
-w-	Write, Delete
--x	Execute
-wx	Write, Delete, Execute
r-x	Read, Execute
rw-	Read, Write, Delete
rwX	Full Access
---	No Access

Note If share-level security is being used in the Windows environment, then only the share passwords affect access. The UNIX permissions have no effect.

Accessing Files Created by NT Clients

Directly mapping NT permissions to UNIX permissions causes some difficulty because NT permissions have a greater level of complexity. UNIX users are unable to use either the `chmod` or `chown` commands to modify the permissions or owners of NT files. The table below shows which UNIX-to-NT file permissions are mapped.

NT	UNIX
R	r
W	w
X	x
D	Ignored
P	Denied
O	Denied

In addition to the permission mappings covered in the previous sections, the following also applies:

- If no ACLs are specified, then the UNIX permission will be `rw-rw-rwx`.
- If the ACL is empty, then the UNIX permissions will be `-----`.
- If the only access allowed by the ACL grants full control to everyone, then the UNIX permissions will be `rw-rw-rwx`.
- In the absence of a group ACL, the owning group will be the user's primary group and the group permissions are set to the same value as the other permissions.

Additionally, if an NT file grants permission to the everyone group (and does not specifically deny access to the owner or the group), then the same access is given to the owner and the primary group. However, UNIX permissions look for explicit permissions for the owner, group, and other. To allow the same level of access in UNIX as NT, these files will have a permission of `r--r--r--`.

Getting Started

3

Using the Command View NAS Web Interface

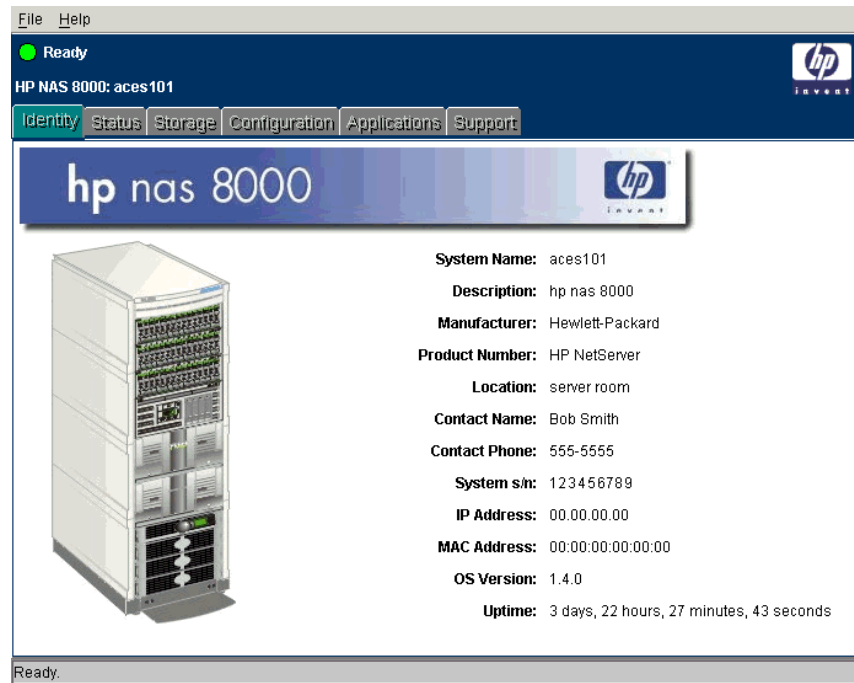
The NAS server and storage array are managed via a web browser. You will perform most administrative tasks with this interface. The Command View NAS requires the Sun Microsystems Java™ Plug-in 1.3.1_01, Standard Edition. Supported browsers include Internet Explorer 5.5 and Netscape 4.77. For more information on supported browser versions for Windows, Solaris, and Linux platforms, see <http://java.sun.com/products/plugin/>. For information on supported browsers for any other platforms, contact your operating system vendor.

Depending on your product configuration, different options display in the Command View NAS web interface.

To access the Command View NAS web interface:

- 1 Start a web browser on a computer on the network.
- 2 Enter the IP address of the HP NAS 8000 in the address or location field. The first time you access the Command View NAS, the Configuration Wizard guides you through configuration. After the initial configuration, an Identity page appears (see Figure 1).

Figure 1 Identity Page



Note If you have trouble connecting, try enabling the browser's option to bypass the proxy server for local addresses.

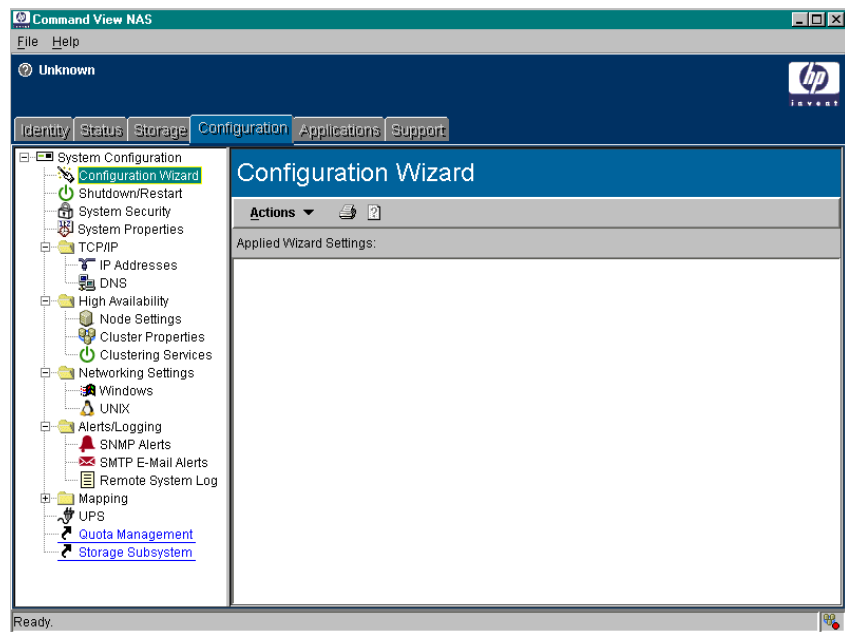
You can click the tabs at the top of the web interface to access the following sections:

- **Identity:** To view general system information
- **Status:** To view overall health of hardware and environmental components on the NAS head and the overall health of any attached storage array; monitor high-availability settings if you have a high-availability NAS server
- **Storage:** To view and manage arrays, LUNS, volume groups, failover packages (if you have a high-availability NAS server), file volumes, directories, data access, snapshots, and quotas

- **Configuration:** To initialize, view, and modify system, network, and alert settings; shutdown/restart the system; set up user and group mapping; configure high-availability settings if you have a high-availability NAS server
- **Applications:** To enable/disable and manage installed software
- **Support:** To contact service and support for the HP NAS 8000; obtain open source code; run diagnostic tools; upgrade the NAS server software; upgrade storage array firmware

When you select any tab other than Identity, a navigation tree appears in the left pane (see Figure 2). A plus sign next to a selection indicates that it contains subentries. To access the subentries, click on the plus sign to expand the tree, or double click on the entry.

Figure 2 Command View NAS



The Command View NAS web interface also lets you perform complex storage array management tasks by launching the Command View SDM.

Make sure you review Command View SDM Limitations before using the software.

Downloading the Sun Microsystems Java™ Plug-In

To launch the Command View NAS, you must have installed the Sun Microsystems Java™ Plug-in 1.3.1_01, Standard Edition. You can download this plug-in if needed as follows:

For Sun Solaris/Windows/Linux


- 1 Go to the Sun Microsystems web site at <http://java.sun.com/products>.
- 2 Select the Java™ 2 Platform, Standard Edition hyperlink.
- 3 Select the appropriate download product and follow the instructions for installation on your system.

The Sun Microsystems web site also has installation instructions for configuring your browser so that it can access the plug-in software.



For HP-UX

For an HP-UX system, go to <http://www.hp.com/products1/unix/java/> and follow the download instructions for the latest version of the Java™ Platform Plug-in.

Using Online Help

You can access the NAS server's online help from the Command View NAS web interface. Click  or the **Help** button in the dialog box windows to access online help. The Command View NAS web interface then opens a top-level help menu. This context-sensitive online help is preloaded on your NAS server.

Help is organized into main-level and sub-level topics. The icon tabs in this help system are:

-  **Contents:** Displays folders and pages that represent the categories of information in the online user's guide. When you click a closed folder, it opens to display its content (subfolders and pages). When you click an open folder, it closes. When you click pages, you select topics to view in the right-hand pane.
-  **Index:** Displays a list of keywords and keyword phrases. These terms are associated with topics in the help system. To open a topic in the right-hand pane associated with a keyword, double-click the keyword.

Printing Help Information

While using the online help, you can print topics and information directly from the viewer. The available print options are determined by the version of your browser.

Click the print icon () and select your print options.

A printable version (PDF format) of all online help, called the *HP Surestore NAS 8000 User's Guide*, is available on your production documentation CD and on the HP support web site at <http://www.hp.com/support/nas8000>.

Task Overview

Prerequisites

During setup, your NAS 8000 was installed and configured by an HP storage specialist who performed these tasks:

- 1 **Planned your network and storage settings.** You should have done this with your HP installation specialist prior to receiving the product. See your HP Surestore NAS 8000 Solution Integration Manual (SIM) Binder for your *Network and Storage Planning Guide* and “Understanding Physical and Logical Storage” on page 21 in this user's guide for more information.
- 2 **Installed the NAS 8000 hardware.** For information, see the *HP Surestore NAS 8000 Installation Guide* in your SIM Binder.
- 3 **Configured your system and network.** For information, see the *HP Surestore NAS 8000 Installation Guide* in your SIM Binder and Configuring Your System and Network on page 43.
- 4 **Set up storage.** For information, see the *HP Surestore NAS 8000 Installation Guide* in your SIM Binder and Managing Your Storage on page 77.

Management Tasks

After the prerequisite tasks are done, you are ready to perform other storage management tasks such as:

- **Configure additional system and network settings** (see Chapter 4, Configuring Your System and Network). You can change these when something about your system changes (location, system administrator, new user or group mappings). See .
- **Manage your storage** (see Chapter 5, Managing Your Storage). Most storage settings were properly set during setup. You will need to change them if you change your storage configuration or if you choose options such as renaming/adding arrays or working with snapshots. Make sure you understand storage concepts before proceeding. See “Understanding Physical and Logical Storage” on page 21 for more information.

- **Monitor your system** by viewing settings on the Status tab (see Chapter 6, Monitoring the System). You'll need to check the status of your system if there is a problem (your system may be set up to automatically notify you of problems).
- **Determine a virus and backup strategy** (see Chapter 7, Enabling Virus and Backup Software). The HP NAS 8000 provides a backup agent, disaster recovery, virus protection, and snapshots functionality to protect your data.
- **Prepare for a disaster** (see Chapter 8, Recovering from a Disaster).
- **Integrate with network backup applications** (see Chapter 9, Integrating with Network Backup Applications).
- **Contact HP support** (see Chapter 10, Obtaining Product Support and Software Upgrades).
- **Upgrade the server software** (see Chapter 10, Obtaining Product Support and Software Upgrades).

Configuring Your System and Network

4

During installation, an HP storage specialist configured your system as part of setup using the web-based Configuration Wizard in the NAS 8000 web interface. (See the *HP Surestore NAS 8000 Installation Guide* in your SIM Binder for information.)

Now you may want to make changes to your settings. You can do so through the Configuration tab, which contains the following configurable parameters:

- **System Properties.** These are informational settings. You can specify the system name, date and time as well as password-protect the administration of your NAS 8000 web interface.
- **TCP/IP Settings.** These settings allow you to set up your device on several network protocols. You enter your IP address and Domain Name Service information here.
- **High Availability.*** You can enter your node settings, name your cluster and Quorum server, set timeouts and intervals, and start and stop clustering services.
- **Networking Settings.** The HP NAS 8000 supports Windows and UNIX networking protocols.
- **Alerts/Logging.** You can enter these optional settings if you want to receive email or server (SNMP) notification in case of a hardware failure or system alert. You can specify a remote server to which you can redirect a copy of the system log.
- **Mapping.** You can map Windows users to UNIX users or Windows groups to UNIX groups.

*This option only appears if you have a high-availability NAS server.

You also can select the UPS connection, manage quotas, modify the storage subsystem, and shut down or restart the device from the Configuration tab.

After you have configured your system to meet your requirements, go to the Storage Tab to arrange the storage space to fit your needs and configure quotas.

Using the Configuration Wizard

The Configuration Wizard automatically appears the first time you connect to the NAS server using a web browser. After that, you can access the wizard to perform guided configuration tasks as follows:

- Open the Command View NAS web interface by typing the IP address in the address or location field of a web browser (you configured this address during installation). The Wizard (shown below) guides you through configuration.
or
- Access the Wizard through the Configuration tab of the Command View NAS web interface by clicking **Configuration Wizard > Actions > Launch Wizard**.

Note Do not use your browser's **Forward**, **Back**, or **Refresh** buttons while the Configuration Wizard is running. Instead use the **Back** and **Next** buttons in the Wizard.

Figure 1 Configuration Wizard



The Wizard lets you:

- Define your system name
- Set the date and time
- Enter your contact information
- Set UPS monitoring
- Specify a password
- View the Command View NAS access list
- Define your TCP/IP addresses
- Enter DNS settings
- Enter your node settings, cluster name, Quorum server name, and timeouts and intervals if you have a high-availability NAS solution
- Set up your Windows (WINS properties and security settings) and UNIX (NIS and NFS settings) environments
- Set SNMP and email (SMTP) alerts
- Enter an address for remote system log data

The Command View NAS web interface also lets you manually configure these settings within the Configuration tab. If your network configuration changes, you need to update these settings.

For specific help on a particular section in the Wizard, click the **Help** button.

Identifying your NAS Server

The first time you access Command View NAS, the Configuration Wizard appears to guide you through configuration. Subsequent times when you access Command View NAS, an Identity page appears and displays the following general system information:

- ***Name** — The system or hostname for your HP NAS 8000
- ***Cluster Name (high-availability configurations only)** — Name of your cluster on your network
- ***Sibling Node (high-availability configurations only)** — The secondary node (server) in your cluster if you have a high-availability NAS server
- **Description** — HP NAS 8000
- **Manufacturer** — Hewlett-Packard Company
- **Product Number** — The product number corresponding to the original configuration of the HP NAS 8000
- ***Location** — The physical location of the HP NAS 8000
- ***Contact Name** — The person to be notified in case of trouble or questions about the HP NAS 8000 (usually the system administrator)
- ***Contact Phone Number** — Usually the phone number of the contact name
- ***Asset Number** — A number that your company might use to identify and track the HP NAS 8000
- **System s/n** — The factory-set serial number of the unit
- ***IP Address** — The IP network address of the Network Interface Card (NIC) in port 1 (although the HP NAS 8000 supports multiple ports, only the first one is displayed)
- **MAC Address** — The unique Machine Address Code for the NIC in port 1
- **OS Version** — The current version of the operating system running on the HP NAS 8000
- **+Array Alias/ID** — The name you gave the array and the array serial number (if you have a SAN configuration, this does not display)
- **Worldwide ID (SAN only)** — Associated ID with the host bus adapter
- **Up Time** — The cumulative up-time of the HP NAS 8000 since the last reboot

*You can change these items from the Configuration tab.

+You can change this from the Storage tab.

Shutting Down and Restarting

Direct-Attached and SAN Configuration

The Shutdown/Restart option applies only to the NAS server. If you need to shut down a direct-attached storage array, shut down the NAS server first.

Shut down the NAS server if you:

- Move the device to a new location
- Anticipate a power outage in your building and you do not have an uninterruptible power supply for the device

Restart the NAS server if you install a new version of the Command View NAS web interface.

Note When restarting the NAS server in a direct-attached configuration, it is not necessary to shut down or restart the storage array.

When shutting down or restarting the server, keep in mind that:

- You and any other connected users will lose the connection to the device.
- The Command View NAS web interface in the current browser cache becomes invalid. The browser closes and you must re-connect to the system after it reboots.

To shut down or restart the device:

- 1 In the Command View NAS web interface, click the **Configuration** tab, then navigate down the tree and select **Shutdown/Restart**.
- 2 Click **Actions > Shutdown/Restart**.
- 3 Select:
 - **Shutdown** if you want to shut down the NAS server completely.
 - **Shutdown/Restart** if you want to shut down and restart the NAS server. If you have installed new firmware, the system will use it on reboot. Wait approximately five minutes for the system to be restored.
- 4 Click **OK**.

High-Availability Configuration

If you have a high-availability NAS server, you have several shutdown options:

- Stop the server and do not fail over packages. You can manually stop each package, then stop the server, or you can stop the server and cause the packages to stop automatically. Once the server is stopped, it is no longer active in the cluster and is not serving any file systems, so you can safely stop it by following steps 1-4 in “Direct-Attached and SAN Configuration” on page 47.
- Fail all packages over to the other server. To do so, simply stop each package and restart it on the other server. Once the packages are all failed over, you can stop the server (take it out of the cluster), then follow steps 1-4 in “Direct-Attached and SAN Configuration” on page 47.
- Fail selected packages over to the other server. This option is similar to the previous option, except that you fail over only selected packages.
- Stop the entire cluster by taking both servers down. You can either manually stop all packages on both servers, then stop the cluster, or simply stop the clustering services to automatically stop all packages. Once the clustering service is stopped, follow steps 1-4 in “Direct-Attached and SAN Configuration” on page 47 on each server.

Configuring System Security

Editing the Command View NAS Access List

The Command View NAS access list allows you to define the machines that may access the Command View NAS web interface. If a specific machine's hostname or IP address is not listed, that machine cannot access the Command View NAS.

To set up the Command View NAS access list:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **System Security**.
- 3 Select **Actions > Edit GUI Access List**.
- 4 Enter the IP address or hostname, then click the add-item icon or press **Enter**.

Setting an Administrative Password

You can set a password for the NAS server. This prevents unauthorized access to the Command View NAS web interface. The NAS server ships without password protection, and the fields are initially blank.

Note If you set a password for the NAS server, protect it as you would any other password. If you forget or lose this password, you will not be able to access your device. Call HP Support for assistance.

If you specify a password, you must know the password to view or modify the information in the other tabs. You can not access the Command View NAS web interface without the password.

To assign, change, or remove an administrative password:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **System Security**.
- 3 Select **Actions > Edit Admin Password**.

4 In the **Current Password** field:

- If you are assigning a password for the first time or if you removed your password, leave this field blank.
- If you are changing or removing the administrative password, enter the current password in this field.

5 In the **New Password** field:

- If you are assigning a password for the first time or changing your password, enter a password in this field. Use any combination of printable characters (ASCII codes 32 through 126) with the exception of \, /, |, !, %, ` (back quote), ' (single quote), and ".
- If you are removing the administrative password, leave this field blank.

6 In the Password Confirmation field:

- If you are assigning a password for the first time or changing your password, confirm the new password by typing it in this field.
- If you are removing the administrative password, leave this field blank.

7 Click **OK**.

8 The next time you access Command View NAS, enter the name “admin” and use the password you created.

Caution If you remove or neglect to assign an administrative password, the Command View NAS web interface will be accessible to anyone who knows its IP address.

Configuring System Settings

Defining the System Name

Note If you have a high-availability NAS server, you must stop clustering services to edit the information.

The system name uniquely identifies your NAS server on your network. It is a text string that contains as many as 15 characters drawn from the alphabet (A-Z), digits (0-9), and minus sign (-). No distinction is made between upper and lower case. However, the name must begin with a letter and the last character must not be a minus sign. The name you use appears on the Identity screen of the web interface and in Network Neighborhood in a Windows networking environment.

To define the system name:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **System Properties**.
- 3 Click **Actions > Edit System Name**. Enter your system name (not the domain) in the **System Name** field. You can use any combination of numbers, letters, or dashes to name your device. However, the name must begin with a letter.
- 4 Click **OK**.

Setting the Date and Time

The NAS server uses the information on this screen to keep track of the date and time for operations such as time stamps for file generation and modification. Failure to set the proper date and time may lead to confusing behavior or misleading time stamping of files and log messages.

To set the system date and time:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **System Properties**.
- 3 Click **Actions > Edit System Time**.
- 4 Select either:
 - **System time** and choose the date and time information.
 - **Network Time Protocol (NTP)** and choose a server with which the NAS 8000 can synchronize system time.
- 5 Click **OK**.

Assigning Contact Information

Some of the **Contact Information** that you enter appears on the Identity screen of the Command View NAS web interface. These items are denoted with an asterisk (*). Network management tools may also function according to the contents of these fields.

To assign contact information:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **System Properties**.
- 3 Click **Actions > Edit Contact Information**.
- 4 Enter the:
 - Name of the person primarily responsible for the NAS server in the ***Contact Name** field
 - Phone number of the person primarily responsible for the NAS server in the ***Contact Phone Number** field
 - Pager number of the person primarily responsible for the NAS server in the **Contact Pager Number** field
 - Email address of the person primarily responsible for the NAS server in the **Contact Email Address** field

- Description of the NAS server's physical location in the ***Location** field.
- Description of the NAS server's specific position on your hardware rack in the **Rack ID** field
- Device's specific location of the rack at your location in the **Rack Position** field
- Number that your company might use to identify and track the NAS server in the ***Asset Number** field

5 Click **OK**.

*Information appears on the Identity screen.

Note

Blank fields do not affect the functionality of the device. However, entering your system location (including rack ID and rack position) lets you easily determine which device has issued an alert when you receive notification of an error. (The email message contains the system name.) If you provide your system location information, you can easily troubleshoot or repair the problem.

Configuring TCP/IP Settings

Defining IP Addresses

Note If you have a high-availability NAS server, you must stop the clustering services to edit the information.

The NAS server has one Network Interface Card (NIC) port on the motherboard and supports two additional slots for NICs. These cards can be either dual-port 10/100 cards or single-port gigabit cards. This support gives the system up to five NIC ports (one on the motherboard and the capacity for a maximum of two dual-port 10/100 NICs).

When you initially set up your NAS server, you need to configure the primary NIC. Connect a laptop to the server management port using a null-modem serial cable, and use terminal emulation software to log in. Access the text interface to manually configure the primary NIC (unless you have Dynamic Host Configuration Protocol [DHCP]). You can use the Command View NAS web interface to configure additional NICs. However, you must first configure the network settings through the serial port or you will not be able to access the HP NAS 8000 through the web-based user interface. See the *HP Surestore NAS 8000 Installation Guide* for more information.

Note DHCP is not supported in high-availability configurations.

The following list shows what BOOTP/DHCP vendor options are supported:

- BOOTP_OPTION_NETMASK
- BOOTP_OPTION_GATEWAY
- BOOTP_OPTION_DNS
- BOOTP_OPTION_DOMAIN
- BOOTP_OPTION_BROADCAST
- BOOTP_OPTION_HOSTNAME
- DHCP_OPTION_WINS
- DHCP_OPTION_LOGSRVS
- DHCP_OPTION_LPRSRVS
- DHCP_OPTION_NTFSRVS
- DHCP_OPTION_XFNTSRVS
- DHCP_OPTION_XDMSRVS

If you have DHCP enabled, NIC configuration occurs automatically. Depending on your configuration, the DHCP server provides any or all of the following parameters: IP Address, Subnet Mask, Gateway Address, Broadcast Address, and DNS Domain Name.

To edit the IP configuration for a NIC port:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **TCP/IP > IP Addresses**. A table lists:
 - NIC Ports and Bond Channels
 - Address configuration (whether it is manual, DHCP or bonded to a bond channel)
 - IP Address
 - Gateway Address
 - Subnet Mask
 - Broadcast Address
 - Management Port
 - MAC Address
 - Card speed
- 3 Select the Port you want to edit then select **Actions > Edit Selected IP Configuration**.
- 4 Select an address configuration (manual or DHCP) from the drop-down list. For a manual configuration, enter the IP Address, Gateway Address, Subnet Mask, and Broadcast Address.
- 5 Click **OK**.

Defining the Command View Management Port

The Command View Management Port lets you define a secure port through which the NAS server and the Command View NAS web interface can communicate. The port is defined by port designation such as eth0 and eth1; it is not defined by IP address. eth0 is *always* the on-board port and is the default management port.

To define the management port you must use the command line interface rather than Command View NAS (see Appendix E, Command View NAS Command Line Interface for directions on accessing the command line interface).

To set the management port:

setSystemManagementNetworkCard ethX

To verify that the management port has been set up correctly:

getSystemManagementNetworkCard

This command will return the name of your management port.

Note

- You will be able to communicate with the Command View NAS only through the designated management port with the IP configuration that you have designated for that port.
- If you change the port to a non-configured port, you will not be able to communicate with the server.

Enabling Bonding

When you configure NIC ports, you may enable bonding through the command line interface rather than Command View NAS (see Appendix E for directions on accessing the command line interface). The bonding mechanism allows for failover of NIC ports when one of the NIC ports fails or abnormally terminates.

To bond the ports take the following steps:

- Configure the first port manually (this can be done through the Command View NAS or using the command line interface)
 - **setNetworkCardIpAddress ethX X.X.X.X** (first parameter is the port designation and second parameter is the IP address).
 - **setNetworkCardBroadcastAddress ethX X.X.X.X** (first parameter is the port designation and second parameter is the broadcast address).

- **setNetworkCardSubnetMask ethX X.X.X.X** (first parameter is the port designation and second parameter is the subnet mask).
- **setNetworkCardGatewayAddress ethX X.X.X.X** (first parameter is the port designation and second parameter is the gateway address).
- Enslave the first port to the bond. The bond will then assume the IP configuration of the first port enslaved.
 - **bondEnslaveNetworkCard ethX bondY** (first parameter is the port being enslaved into the bond that is designated by the second parameter).
- Enslave the second port to the bond.
 - **bondEnslaveNetworkCard ethY bondY** (first parameter is the port being enslaved into the bond that is designated by the second parameter).

To un-bond the ports take the following steps:

- **bondReleaseNetworkCard ethY bondY** (first parameter is the port being un-bonded from the bond that is designated by the second parameter).

Note The ports are being un-bonded in the reverse order that they were enslaved.

- **bondReleaseNetworkCard ethX bondY** (first parameter is the port being un-bonded from the bond that is designated by the second parameter)
- Reboot the NAS server.

Setting the Domain Name Service (DNS)

Domain Name Servers convert system names that people can remember (such as nas8000.fc.hp.com) to IP addresses (such as 123.45.67.89) that are used by packet-routing software.

To enter the DNS information:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **TCP/IP > DNS**.
- 3 Select **Actions > Edit DNS Values**.
- 4 If required, enter the **DNS Domain Name**. The NAS server can belong to only one domain.
- 5 Enter **DNS IP Addresses**, pressing **Enter** after each address (up to a maximum of three). You can enter them in the appropriate search order (that is, enter the IP address of the Primary DNS first, followed by the IP address of the secondary DNS, and so on until all of your Domain Name Servers are identified) or rearrange them afterward using the up and down arrow buttons.
- 6 Click **OK**.

To edit the DNS information, click **Actions > Edit DNS Values**, then:

- Click the incorrect entry to modify it.
- Click the entry and click the delete icon to remove it.

Click **OK** to apply each change.

Configuring High-Availability Settings

Cluster Configuration Overview

Note This section applies only if you have purchased a high-availability NAS solution.

You must configure your cluster. Follow these steps in order.

Task...	Details...
1. Preliminary node configuration	See the <i>HP NAS 8000 High-Availability Server Installation Guide</i> in your SIM Binder.
2. Define the cluster	<p>After you complete the minimum network configuration on both of the cluster nodes (servers), you can define the cluster. Defining the cluster consists of:</p> <ul style="list-style-type: none">■ specifying cluster nodes and selecting the NICs to be used for cluster heartbeats (see “Entering Node Settings” on page 61)■ naming the cluster (see “Defining the Cluster Name” on page 62)■ specifying the Quorum server (see “Defining the Quorum Server” on page 62) <p>You can perform this configuration from one node. You do not need to repeat it on the other node. After you apply the cluster configuration (the last step in defining the cluster), the settings are automatically mirrored to the other cluster node. (The Configuration Wizard applies the configuration automatically. If you are using the Command Line Interface, use the <code>applyClusterConfiguration</code> command.)</p>
3. Activate clustering services	See “Starting and Stopping Clustering Services” on page 64.

Task...	Details...
4. Configure the node	You can now complete the balance of the node configuration on each node. The cluster can be either up or down. A defined cluster allows subsequent node configuration to be synchronized between the nodes (assuming that they are available on the network).
5. Configure the storage	<ol style="list-style-type: none"> 1 Create volume groups. (See “Creating a Volume Group” on page 82.) 2 Assign volume groups to packages and start packages to activate volume groups. (See “Adding a New Package” on page 86.) <p>Create file volumes and shares on the active volume groups. (See “Creating a New File Volume” on page 92 and “Creating or Editing an SMB Share” on page 96 or “Creating or Editing an NFS Export” on page 97.)</p>
6. Configure the package	<ol style="list-style-type: none"> 1 Name the package. 2 Specify the primary owner (which node will “own” the package). 3 Assign volume groups to the package. 4 Specify virtual IP addresses for the package. 5 Apply the package configuration. 6 Start the package (if desired). <p>See “Adding a New Package” on page 86.</p>
7. Activate the package	See “Starting a Package” on page 88.

For more information about concepts related to this material, see “Understanding High Availability” on page 24.

Entering Node Settings

Note This section applies only if you have purchased a high-availability NAS solution.

Before you proceed, you must stop the clustering services to edit the information.

You initially enter your node settings in the Configuration Wizard. The node settings let you configure the two nodes (servers) in your cluster. Each server has one or more network interface cards that can be selected to provide cluster heartbeats. A heartbeat is a periodic signal generated by the server to indicate that it is still running. You can have multiple NICs for heartbeats for each server but only one heartbeat exists for each specified NIC.

To enter node settings:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **High Availability**, then select **Node Settings**.
- 3 Select **Actions > Change Node Settings**.
 - Enter the **Node Names**. This is the hostname of each server that will be a member of the cluster. Hostnames are limited to 40 characters and cannot contain spaces, forward slash (/), backslashes (\), or asterisks (*).
 - If you want to start the clustering services after a reboot, check the box.
 - Select the **Heartbeat NICs**. A table lists the NICs that are already used for heartbeats and ones that are available. From the available NICs list, select the NICs to use as a heartbeat, then click **Add**. NICs that are used as heartbeats can still be used for accessing storage. Note that both nodes in the cluster will use these heartbeat settings.
- 4 Click **OK**.

From the **Actions** button, you can also:

- Delete the cluster configuration
- Specify which node to start or stop

Defining the Cluster Name

Note This section applies only if you have purchased a high-availability NAS solution.

Before you proceed, you must stop the clustering services to edit the information.

The cluster name identifies your cluster on your network. It is a text string that is limited to 40 characters and cannot contain spaces, forward slash (/), backslashes (\), or asterisks (*).

To name a cluster:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **High Availability**, then select **Cluster Properties**.
- 3 Select **Actions > Edit Cluster Name**.
- 4 In the **Cluster Name** field, type a name for the cluster.
- 5 Click **OK**.

Defining the Quorum Server

Note This section applies only if you have purchased a high-availability NAS solution.

Before you proceed, you must stop the clustering services to edit the information.

Enter the name (up to 32 characters) or IP address of the host system that is acting as the Quorum server for the cluster. A Quorum server is a failover mechanism that acts as a cluster arbitrator between the NAS servers in your cluster. It prevents the formation of multiple clusters that aren't aware of one another but are accessing the same storage. It is not a physical part of the cluster.

To define a Quorum server:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **High Availability**, then select **Cluster Properties**.
- 3 Select **Actions > Edit Quorum Server Name**.

- 4 In the **Quorum Server** field, type the hostname for the Quorum server on your network.
- 5 Click **OK**.

Setting Timeouts and Intervals

Note This section applies only if you have purchased a high-availability NAS solution.

Before you proceed, you must stop the clustering services to edit the information.

The values you set on this screen let you determine the rate at which problems on the NAS server are detected. You can set timeouts and intervals for the Quorum server, heartbeat, and network-failure detection. Recommended values appear automatically in the fields.

Keep in mind:

- If you enter low values, problems will be detected sooner but susceptibility to high network traffic will be greater.
- If you enter high values, problems will not be detected quickly but false failovers will occur less frequently.

To edit timeouts and intervals:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **High Availability**, then select **Cluster Properties**.
- 3 Select **Actions > Edit Timeouts and Intervals**.
- 4 Enter values in minutes and seconds in the following fields:
 - **Quorum Server Polling Interval:** Time between polling attempts between a cluster node and the Quorum server.
 - **Heartbeat Interval:** Time between heartbeat messages from one cluster member to another. This value should be at least half of the Node Timeout value.
 - **Network Polling Interval:** Interval for polling the network interfaces for link status to determine that they can still send and receive data. This value determines how quickly network failures are detected.

- **Node Timeout:** Timeout value for a heartbeat between nodes. If a heartbeat is not detected for this specified amount of time, the node awaiting/monitoring the heartbeat will determine that the node is unavailable and will commence cluster reformation and package failover.

5 Click **OK**.

Starting and Stopping Clustering Services

Note This section applies only if you have purchased a high-availability NAS solution.

Once a cluster configuration exists, you can manually start clustering services. The cluster will not start automatically. You can start the clustering services with or without packages defined. The clustering services will automatically start any packages that you configured with Auto Start enabled. See “Adding a New Package” on page 86 for more information on configuring packages.

When you stop the clustering services, all packages stop gracefully and the cluster stops. Stopping clustering services does not cause the systems to shut down or reboot. Upon completion of a clustering services stop command, the systems will be up but no packages will be running; therefore, all volume groups will be inactive and no storage will be accessible to client systems.

You can configure the clustering services to automatically start when the system boots. By default, the clustering services auto-start feature is disabled and you must start clustering services manually. If you enable clustering services auto-start, clustering services will start automatically when the system boots. When you modify the clustering services auto-start setting, the setting will be mirrored on the other cluster nodes. See “Entering Node Settings” on page 61 if you want to change the auto-start feature.

The Start/Stop Clustering Services screen allows you to turn clustering capabilities on or off. You must stop clustering services to change configuration information on your NAS server. Once you stop clustering services, you will be able to access your data through the physical IP address but not the virtual IP address.

Caution All current connections to CIFS and NFS will be lost when you stop clustering services.

To start or stop clustering services:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **High Availability**, then select **Cluster Services**.
- 3 Select:
 - **Actions > Start Clustering Services**. You will not be able to select this item if the clustering services have already been started.
 - **Actions > Stop Clustering Services**. You will not be able to select this item if the clustering services have already been stopped.

Configuring Networking Settings

Windows Settings

Specifying WINS Properties

Similar to DNS, the Windows Internet Naming Service (WINS) is the Windows NT server method for associating a computer's hostname with its address.

To specify the WINS properties:

- 1 In the Command View NAS web interface, click the **Configuration** tab, navigate down the tree to **Networking Settings > Windows**.
- 2 Select **Actions > Edit WINS Properties**.
- 3 Enter a **WINS Server IP Address**.
- 4 Optionally, you can enter a **Network Neighborhood Comment** (the comment you enter appears in the Network Neighborhood comment field).
- 5 Click **OK**.

Defining Windows Security

You can choose from two Windows NT security modes:

- **Share-Level Security:** The NAS server handles its own security. Shares may be password-protected and may limit your access (read-only and/or read/write) to data. You may define a password when you create the share.
- **User-Level Security:** A domain controller is used to authenticate users when they access the NAS server. This requires specifying the domain name.

To define the Windows NT security mode:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **Networking Settings > Windows**.
- 3 Select **Actions > Edit Windows Security Properties**.

4 Select either:

— **Share Level Security:**

Specify the Workgroup to which the NAS server belongs.

— **User Level Security** (see your system administrator for the following Windows security information):

- a Enter the **Domain** name. The system administrator must have already created an account for the NAS server in the domain you choose to join. This is on the planning worksheet in your SIM binder.
- b Enter the name or IP address for the **Primary Domain Controller** (PDC).
- c Enter the correct **User Name** and **Password** for the administrator of the PDC.
- d Enter the hostname or IP address for any **Backup Domain Controllers** (BDC) used in your network. BDCs are generally set up by your network administrator.

5 Click **OK**. The NAS server attempts to join the domain. The NAS server will fail in its attempt to join the domain if the Windows domain controller does not have an account for the NAS server.

Note

If you need to rejoin a Windows domain that the NAS server had previously joined, you might need to reset or remove and add the NAS server on the Windows domain controller that the NAS server will attempt to rejoin.

UNIX Settings

Specifying NIS Properties

The NAS server supports Network Information System (NIS). NIS maintains a central database of names and locations of resources on a network. NIS was formerly known as Yellow Pages.

To enable or disable NIS:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **Networking Settings > UNIX**.
- 3 Select **Actions > Edit NIS Properties**.
- 4 Check **Disable NIS** or **Enable NIS** (**Disable NIS** is the default).
- 5 If you are enabling NIS:
 - a Enter the NIS domain name in the **Domain Name** field.
 - b Select either:
 - **Broadcast to locate Server at boot time**. In order for the NAS server to find the NIS server, the server must be on the same subnet as the NAS server.
 - **Specify server** and enter the master server's IP address.
- 6 Click **OK**.

Specifying NFS Properties

Network File System (NFS) settings are optional. NFS is a client/server application that lets a user view and optionally store and update files on a remote computer as if the files were on the user's own computer.

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **Networking Settings > UNIX**.
- 3 Select **Actions > Edit NFS Properties**.
- 4 You can change the number of **Network File System Daemon (NFSD)** processes. This value, which specifies the number of NFSD processes that are created on the NAS device, takes effect immediately; NFS restarts with the new number of daemons. This setting has a direct effect on NFS performance.
 - A small number of NFSD process (for example, a value of 1) can support many NFS clients, but it must provide sequential service. This limitation can create performance problems if more than one NFS client tries to access the NAS device.
 - A large number of NFSD processes can support the same number of NFS clients, but they do so in parallel, thus increasing the performance for the clients. The more NFSD processes you have, the more system resources are used. Specifying a large value can result in poor performance.
You can use a minimum value of 10 and a maximum value of 128. If you are you using your NAS device primarily as an NFS server, HP recommends that you increase the value of this setting.
- 5 Enter the IP address or hostname of any host where you want to grant root access privileges.
- 6 Click **OK**.

You do not need to restart the system.

Configuring Alert Settings

Defining SNMP Alerts

If you are using a network management product such as HP OpenView, CA Unicenter, or Tivoli Network Node Manager, you can define the names of management workstations to receive notification in case of a failure. For more information about these products, see the *HP Surestore Enterprise Integrations Installation and User Guide* at <http://www.hp.com/support/emsp>.

Note The information on this screen is optional. Blank fields do not affect the functionality of the device. In the event of a hardware failure or system alert, messages are sent through SMTP (email), or they are logged in the system log.

To define the management servers to notify:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **Alerts/Logging**, then select **SNMP Alerts**.
- 3 Select **Actions > Edit SNMP Settings**.
- 4 Enter the SNMP password required for network management tools to retrieve operational or configuration information from the device in the **SNMP Community String** field.
- 5 Enter the name or IP address of the server you want the system to notify in the **SNMP Trap Destinations** field.
- 6 Click **OK**.

To edit the Trap Destinations, click **Actions > Edit SNMP settings**, then:

- Click the incorrect entry to modify it.
- Click the entry and click the delete icon to remove it.

Click **OK** to apply each change.

See Appendix B, SNMP Trap Definitions for a list of the traps sent by the NAS server.

Defining Email Alerts (SMTP)

The NAS server lets you automatically notify individuals via email if there is a hardware failure or a critical system alert.

Note The information on this screen is optional. Blank fields do not affect the functionality of the device. In the event of a hardware failure or system alert, messages are sent through the network management tool or they are logged in the system log.

To set up automatic notification:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **Alerts/Logging**, then select **SMTP Email Alerts**.
- 3 Select **Actions > Edit SMTP Values**.
- 4 Enter the name of the email server in the **SMTP Server Name** field. The email server must be an IP address or a fully qualified name (such as alpha.corp.com). You must specify an email server if you want to define one or more email recipients.
- 5 Click **Add** and enter the email address that should receive alerts. Click **OK**. Click **Add** for any additional email addresses you want to add. You can also:
 - Edit an existing email by selecting it from the table and clicking **Edit**.
 - Delete an entry by selecting it from the table and clicking **Delete**.
- 6 Click **OK**.
- 7 You can send a test email to make sure your settings are correct by selecting the recipient from the list and clicking **Actions > Send test email to selected address**.

See Appendix B, SNMP Trap Definitions for a list of the traps sent by the NAS server.

Setting Up the Remote System Log

You can redirect a copy of the system log to a specified server. This redirection lets you manage a central location for the event log instead of working with different interfaces or systems.

Note To receive the log messages from the NAS server, you must enable remote system-log capabilities on your UNIX system. First, add the `-r` option as part of the `syslogd` daemon's startup parameter. Then, restart the `syslog` service. You also need to plan for the appropriate amount of log space on your UNIX system. See your operating system documentation for additional help in modifying your `syslogd` daemon parameters.

To define a server to receive the remote system log:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **Alerts/Logging**, then select **Remote System Log**.
- 3 Select **Actions > Edit Remote Server**.
- 4 In the **Remote UNIX System Log Address** field, enter the name or IP address of the remote server to which you want to redirect the system log. (If the field is left blank, this feature is disabled.)
- 5 Click **OK**.

Note Remote System Log information is optional. A blank field does not affect the functionality of the device.

If a monitored environmental item or activity is running out of specification, an alert/trap is sent to the remote system log.

See Appendix B, SNMP Trap Definitions for a list of the traps sent by the NAS server.

Configuring User and Group Mapping

Understanding User and Group Mapping

This screen lets you map Windows users/groups, who use the Server Message Block Protocol/Common Internet File System protocol (SMB/CIFS), to UNIX users/groups, who use the Network File System protocol (NFS):

- **SMB/CIFS**, the Windows protocol for sharing files, lets client applications read and write to files. CIFS is a standard protocol that lets programs request files and services on remote computers over the internet. CIFS uses the client/server programming model. A client program makes a request of a server program (usually running on another computer) for access to a file or to pass a message to a program that runs on the server computer. The server takes the requested action and returns a response.
- **NFS**, the UNIX protocol for sharing files, is a client/server application that lets a user view and optionally store and update files on a remote computer as though they were on the user's own computer.

Note User or group mapping is available only when you select user-level security on the Windows Security screen. User or group mapping using names is most useful when NIS is enabled.

The NAS server maintains a mapping of users/groups between the two protocols. If a Windows user/group is not mapped to an existing UNIX user/group ID, then when the Windows user/group accesses the NAS server for the first time, a new UNIX user/group ID is generated and the Windows user/group is mapped to it.

Mapping users/groups improves:

- Adherence to file and directory permissions
- Compliance to disk quotas
- Display of file and directory ownership

To set up user or group mapping:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **Mapping**, then select **User Mapping** or **Group Mapping**. A table displays the current mappings of Windows to UNIX users/groups.
- 3 Select **Actions > Add User Mapping Entries** or **Add Group Mapping Entries**.
- 4 In the Windows user or group domain section, select a domain from the drop-down list, then select a user or group from the list.
- 5 In the UNIX user or group name section, select a user or group from the drop-down list.
- 6 Click **Add**. Repeat steps 4-6 for all the users or groups you want to map.
- 7 Click **OK**.

To unmap an entry:

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the System Configuration tree to **Mapping**, then select **User Mapping** or **Group Mapping**.
- 3 Select the entry you want to unmap.
- 4 Select **Actions > Delete Selected User Mapping** or **Delete Selected Group Mapping**.
- 5 Click **OK** to unmap the entry.

Importing and Exporting Users or Groups

In addition to setting up user/group mapping, you can export a list of Windows and UNIX users/groups, which might help you map users/groups. Also, you can import or export a user/group map file. Importing a user/group map lets an unlimited number of mappings occur simultaneously. Exporting a user/group map lets you save the map for later use or for disaster recovery.

Follow the directions below to:

- Import/export a user or group map file
- Export a list of Windows and UNIX users or groups

Note Group mapping is similar to user mapping where you associate or “map” a group using SMB/CIFS file protocol to a group using the NFS file protocol.

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **Mapping**, then select **User Mapping** or **Group Mapping**.
- 3 Select **Actions** > then one of the following options:
 - **Import User Map** or **Import Group Map**. A window appears. Find the location for the user map you've created. Click **Open** to import the file to the NAS server. All entries will be merged; that is, new entries will be added, and old entries will be remapped.
 - **Export User Map** or **Export Group Map**. Specify the location and file name, then click **Save**.
 - **Export User List** or **Export Group List**. Specify the location and file name of the export list, then click **Save**.

Configuring UPS Connections

If you connected an optional UPS to your NAS server during installation, the NAS server attempts to communicate with the UPS through a serial connection.

To set up and monitor a UPS connection for your NAS server:

- 1 The APC UPS has only one serial port. The NAS server, however, has two ports. Connect the UPS serial port to the COM1 port on the back of the NAS server. See the *HP Surestore NAS 8000 Installation Guide* for more detailed information.
- 2 In the Command View NAS web interface, click the **Configuration** tab.
- 3 Navigate down the tree and select **UPS**.
- 4 Select **Actions > Edit UPS Setting**.
- 5 Select the appropriate UPS, then click **OK**.

After you make the connections and configure the device, the NAS server:

- Monitors the status of the UPS. If the UPS ever defaults to battery power, the system reports the status as an event, which is passed along to a management station as an SNMP trap.
- Manages a graceful shutdown of the server and the storage array in the event that the battery runs too low.

For further information about the UPS, see:

- “Viewing UPS Status” on page 122
- “UPS Upgrade” on page 195

Managing Your Storage

5

To set up your storage, you need to implement your plan. You do so in the Storage tab.

Note You must completely configure your NAS server before you attempt to set up your storage. For more information, refer to the *HP Surestore NAS 8000 Installation Guide* or access the Configuration Wizard in the Configuration tab.

In the Storage tab, you must:

- Create Logical Unit Numbers (LUNs). A unique number that identifies a specific unit of storage, a LUN logically organizes physical disk space for storage use. You can have one or more LUNs on the array depending upon your storage requirements. If you have a SAN, you can not create LUNs.
- Aggregate your LUNs into one or more volume groups. Volume groups can span several LUNs, even those that are on separate arrays.
- Partition your volume groups into file volumes.
- Create directories and sub-directories beneath your file volumes to further organize your data.
- Make file volumes or directories available to users by sharing or exporting them.

You can also:

- View, scan for, and rename arrays
- Manage failover packages (if you have a high-availability NAS server)
- Create, edit, delete, and schedule snapshots
- Configure user quotas
- Configure group quotas

Managing Arrays and LUNs

Viewing the Storage Array Summary

The Storage Array Summary page displays a table that lists the storage array attached to the NAS server and information about its storage configuration.

To examine and manage the storage you have available:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Storage Array Summary**.

A table displays the following drive information for the storage you have available:

Column	Description
Array Identifier	Name you gave the array (see “Renaming an Array” on page 79) or default vendor product number/serial number. Click on the plus sign to expand the entries. If you have a: <ul style="list-style-type: none">■ VA7100 array, one redundancy group and the LUNs you created are displayed■ VA7400 series array, the redundancy groups and the LUNs in those redundancy groups are displayed If you have a SAN, this column lists the LUNs that were found.
Total Physical Capacity	Total physical storage space.
Capacity Allocated to LUN(s)	Usable space allocated to a LUN.
Capacity Available for LUNS(s)	Space available after you create LUNs.
RAID Redundancy	Space the system needs for RAID overhead.
Active Spare Capacity	Reserved drive space available in case a drive fails.
Unincluded Capacity	Drive space that isn't recognized by the NAS server because drive: <ul style="list-style-type: none">■ Belongs to a different array■ Is not formatted correctly This space will not be used until you resolve the issue.

You can click on a column heading to sort items in that column. The **Actions** button in the upper left corner lets you:

- Scan for a new storage
- Rename an array
- Launch the array user interface for advanced array management
- Create a new LUN
- Delete the selected LUN

Note If you have a SAN, you can only scan for new storage. The other topics are grayed out.

You can also refresh the items in your display by selecting **Actions > Refresh**.

Scanning for New Storage

If you attach a new array, you must scan for the new array and the array's LUNs to make them accessible. (If you have a SAN, you cannot add or delete LUNs from this interface.) This process may take a few minutes. Restarting your device also scans for new storage.

To scan for new storage:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Storage Array Summary**.
- 3 Select **Actions > Scan for New Storage**.

Renaming an Array

Note If you have a SAN, disregard this topic.

To rename an array:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Storage Array Summary**.
- 3 Select the array you want to rename by clicking in the row.
- 4 Select **Actions > Rename Array**.
- 5 A dialog box appears. Type a new name.
- 6 Click **OK**.

Using Advanced Array Management

Note If you have a SAN, disregard this topic.

Advanced Array Management lets you do the following for the array(s) attached to the NAS server:

- View data resiliency
- Modify RAID levels (the default is AutoRAID)
- Enable or disable active spare mode
- Automatically include and format new drives

If you select this option, the Command View SDM web interface is launched. See “Command View SDM Limitations” on page 213 for more information.

To manage arrays:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Storage Array Summary**.
- 3 Select **Actions > Advanced Array Management**.

Creating a LUN

Note If you have a SAN, disregard this topic because you can not create LUNs.

The Create New LUN dialog box displays the array's available capacity for creating a LUN.

The minimum number of LUNs per array is one. The HP NAS 8000 supports a maximum of 127 LUNs.

To create a LUN:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Storage Array Summary**, then select a storage array.
- 3 Select **Actions > Create New LUN**.

- 4 The Create New LUN dialog box appears. If you have a:
 - VA7100 array, select a LUN number from the drop-down list and enter the LUN size.
 - VA7400 series array, select a redundancy group from the drop-down list, select a LUN number from the drop-down list, and enter the LUN size.
- 5 Click **OK**.

Once you have created a LUN, you are ready to create a volume group.

Deleting a LUN

Note If you have a SAN, disregard this topic because you can not delete LUNs.

To delete a LUN:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Storage Array Summary**, then select a storage array.
- 3 Select the LUN you want to delete by clicking the row.
- 4 Select **Actions > Delete Selected LUN**.
- 5 Click **OK**.

Note You cannot delete a LUN if it is part of a volume group. You must first delete the volume group.

Managing Volume Groups

Viewing Volume Groups

A volume group is made up of one or more LUNs.

To view the volume group:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree and select **Volume Groups**.

A table displays the following drive information for every volume group:

- Name
- Capacity
- Allocated space assigned from a volume group to one or more file volumes
- Space available in the volume group for file volume creation

You can click on a column heading to sort items in that column. The **Actions** button in the upper left corner lets you create, edit, and delete volume groups. You can also refresh the information in the table by selecting **Actions > Refresh**.

Once you have created a volume group, you are ready to create new file volumes.

Creating a Volume Group

Before you can create a volume group, you must first create one or more LUNs.

To create a new volume group:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree and select **Volume Groups**.
- 3 Select **Actions > Create New Volume Group**.
- 4 Enter a name for the volume group.
- 5 From the available LUNs list, select the LUN to add to the volume group, then click **Add**. You can add as many LUNs as are available to the volume group.

6 Click **OK** to create the new volume group.

You are now ready to create file volumes and place data in those volumes.

Note If you have a high-availability NAS solution, you must assign the volume group to a package before you can perform any further storage configuration. The *only* way to activate a volume group is to start the package to which you have assigned the volume group.

Editing a Volume Group

The Edit Volume Group dialog box lets you:

- Rename a volume group
- Extend the size of an existing volume group

To edit a volume group:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree and select **Volume Groups**.
- 3 Select the volume group you want to rename by clicking the row.
- 4 Select **Actions > Edit Selected Volume Group**.
 - To rename a volume group: Enter a new name for the volume group in the dialog box.
 - To extend the size of the volume group: A table lists the LUNs that are already a part of the volume group and ones that are available. From the available LUNs list, select the LUN to add to the volume group, then click **Add**. You can add as many LUNs as are available to the volume group.
- 5 Click **OK**.

Note You cannot de-allocate LUNs that are already a part of the volume group.

Deleting a Volume Group

Before you delete a volume group, you must first delete any file volumes or snapshots associated with the volume group.

Note If you have a high-availability NAS solution, before you delete the volume group, you must first stop and delete the package that contains the volume group.

To delete a volume group:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree and select **Volume Groups**.
- 3 Select the volume group you want to delete by clicking the row.
- 4 Select **Actions > Delete Selected Volume Group**.
- 5 Click **OK** to delete the volume group.

Managing Failover Packages

Viewing Failover Packages

Note This section applies only if you have purchased a high-availability NAS solution.

All storage is controlled by packages. Packages are the smallest units of failover in the cluster. In other words, if a package resource (storage or network) fails, the package will be failed over to another node. Each package and its associated resources are monitored independently. This allows failures that are limited to a single package to be handled without affecting the state of other packages.

To view failover packages:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree and select **Failover Packages**.

A table displays the following information for every failover package:

Column	Description
Package Name	A string of 40 characters that cannot include spaces, forward slash (/), backslashes (\), or asterisks (*). Identifies the package when you view its status or operate or modify it.
Package Status	Displays whether the package is starting, has stopped, has failed over, or is inactive.
Failback Policy	<p>The Failback Policy is used when the package is not running on its primary server even though the primary server is capable of running the package.</p> <ul style="list-style-type: none">■ If you set the Failback Policy to Automatic, the package will always attempt to move back to the primary server.■ If you set the Failback Policy to Manual (default), the package will not change servers until you manually fail it back.
Auto Start	Enabled or disabled. If Auto Start is enabled, the package automatically starts once the server is running on the cluster.

Column	Description
Reboot on Failure	Enabled or disabled. If Reboot on Failure is enabled and a failure occurs, the server automatically reboots.
Primary Node	Hostname of the NAS server that is designated as the owner of the package. Under normal circumstances, the primary node (server) should start the package by default. This name is selected from the list of cluster members or nodes specified in the cluster configuration.
Volume Groups	Volume groups that the package maintains.
Virtual IP Addresses	IP addresses that will be used to access the volumes specified in the package. You can have multiple IP addresses, but at least one must be specified. The virtual IP address will become the “well known” address for accessing the volumes in the package.

You can click on a column heading to sort items in that column. The **Actions** button in the upper left corner lets you add, edit, delete, start, or stop a package as well as manually fail over or fail back a package. You can also refresh the information in the table by clicking **Actions > Refresh**.

Adding a New Package

Note

- This section applies only if you have purchased a high-availability NAS solution.
- You must enter all of the high-availability information in the Configuration tab before creating a new failover package.

To add a new package:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree and select **Failover Packages**.
- 3 Select **Actions > Add New Package**.
- 4 Enter a **Package Name**. Package names are limited to 40 characters and cannot contain spaces, forward slash (/), backslashes (\), or asterisks (*).
- 5 Select a **Failback Policy** from the drop-down list.
- 6 Check **Auto Start** if you want the package to automatically start once the server is running in the cluster.

- 7 Check **Reboot Node on Failure** if you want the server to automatically reboot if a failure occurs.
- 8 Select a **Primary Node** that you want to start the package from the drop-down list.
- 9 From the **Available Volume Groups** list, select the volume group(s) you want to include in the package, then click **Select**.
- 10 Enter a **Virtual IP Address** (an IP address used to access the storage associated with the package) and enter the **Subnet**. Click **Add**.
- 11 Click **OK**. To activate the package, you must start it. See “Starting a Package” on page 88 for information.

Editing a Package

Note This section applies only if you have purchased a high-availability NAS solution.

Before you proceed, you must stop the package to edit the information.

To edit a package:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree and select **Failover Packages**.
- 3 Select **Actions > Edit Package**.
- 4 Select a **Failback Policy** from the drop-down list.
- 5 Check **Auto Start** if you want the package to automatically start once the server is running in the cluster.
- 6 Check **Reboot Node on Failure** if you want the server to automatically reboot if a failure occurs.
- 7 Select a **Primary Node** from the drop-down list.
- 8 From the **Available Volume Groups** list, select the volume group you want to include in the package, then click **Select**.
- 9 Enter a **Virtual IP Address** (an IP address used to access the storage associated with the package) and enter the **Subnet**. Click **Add**.
- 10 Click **OK**. To activate the package, you must start it. See “Starting a Package” on page 88 for information.

Deleting a Package

Note This section applies only if you have purchased a high-availability NAS solution.

Before you proceed, you must stop the package to edit the information.

Deleting a package does not delete the volumes and shares/exports within the package. However, once the package is deleted, the volumes within the deleted package will not be accessible to client systems until you add them to another package.

To delete a package:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree and select **Failover Packages**.
- 3 Select the package you want to delete by clicking the row.
- 4 Select **Actions > Delete Package**.

Starting a Package

Note This section applies only if you have purchased a high-availability NAS solution.

This operation runs the specified package on the designated server. Once the package is up, the volumes in the package are mounted and the shares and exports associated with each volume are accessible to client systems. Execute **Start Package** after you create a package or when you want to restart a package that has been stopped.

To start a package:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree and select **Failover Packages**.
- 3 Select the package you want to start by clicking the row.
- 4 Select **Actions > Start Package**.
- 5 Select the **Node** where you want the package to start from the drop-down list.
- 6 Click **OK**.

Stopping a Package

Note This section applies only if you have purchased a high-availability NAS solution.

The file system services, NFS, and CIFS are temporarily stopped; the volumes within the package are unmounted; and NFS and CIFS are restarted. Once the package has been stopped, it can be restarted on any active server in the cluster. After a package is stopped, the volumes within the package are no longer available to client systems until the package is restarted. Stopping a package does not affect the server's cluster status and does not cause the cluster to go down.

Caution Check the Client Activity page before stopping the package to make sure no one is accessing it. Stopping a package disrupts service to users who are accessing the package(s) through the virtual IP address. After you restart the package, the virtual IP address is valid again.

To stop a package:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree and select **Failover Packages**.
- 3 Select the package you want to stop by clicking the row.
- 4 Select **Actions > Stop Package**.

Failing Over a Package

Note This section applies only if you have purchased a high-availability NAS solution.

The specified package fails over to another server in the cluster. The failover consists of stopping the package on the primary server (node), then starting the package on the secondary server. This action does not affect the designated ownership of the package. In other words, the primary node specified in the package configuration doesn't change. If the cluster were stopped and restarted, the package would automatically migrate back to its primary node. This action provides a mechanism for manually failing over packages without requiring a failure condition. One use of this functionality is to allow manual load-balancing without requiring the cluster or individual nodes to be reconfigured and/or rebooted.

A package failover involves both stopping the existing package on one node and starting the new instance of the package on the other node.

You would manually fail over a package when:

- You need to take the primary server down for moving, cleaning, or service.
- You want to transfer a package to the secondary server.

To fail over a package:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree and select **Failover Packages**.
- 3 Select the package you want to fail over by clicking the row.
- 4 Select **Actions > Manually Fail Over Package**.

Failing Back a Package

Note This section applies only if you have purchased a high-availability NAS solution.

If you set a package to **Manually Failback** and the primary node goes down, the package remains on the adoptive node until it is manually failed back.

To fail back a package:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree and select **Failover Packages**.
- 3 Select the package you want to fail back by clicking the row.
- 4 Select **Actions > Manually Fail Back Package**.

Managing File Volumes

Viewing File Volume Information

File volumes are the basic unit of logical storage for a file system on the NAS server. You create file volumes by allocating space in a volume group. Therefore, before you can create a file volume, you must create a volume group.

After you have created file volumes, you can create directories under the new file volumes to organize your data.

To view summary information on all file volumes that exist on your NAS server:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **File Volumes**, then select **File Volumes Summary**.

A table displays the following information for every file volume:

- File volume name
- Volume group the file volume is a part of
- Amount of total capacity of the file volume
- Amount of space actually used by each volume
- Amount of free space available within each volume
- Notification threshold
- Whether quotas are enabled or disabled
- Number of snapshots defined for each file volume
- Number of shares defined for the file volume level

You can click on a column heading to sort items in that column. The **Actions** button in the upper left corner lets you to create, edit, and delete file volumes. From the **Actions** button you can also create a new snapshot or refresh the information in the table by selecting **Actions > Refresh**.

Creating a New File Volume

File volumes are the basic unit of storage for a file system on the NAS server. In order to create file volumes, you must already have created one or more volume groups.

To create a new file volume:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **File Volumes**, then select **File Volumes Summary**.
- 3 Select **Actions > Create New File Volume**.
- 4 Select a volume group from the pull-down menu.
- 5 Enter a new **File Volume Name**.
- 6 Enter the desired file volume **Capacity**.
- 7 Check whether you want quota management enabled. Quotas allow you to restrict the space usage on your system for both users and groups.
- 8 When you store data in your new file volume, the available space decreases. To send an SNMP alert when the used space on a volume reaches a certain percentage, select a percentage from the **Send Notification at** drop-down list. **Note:** This percentage is used in conjunction with the settings you entered on the SNMP alert, email, and Syslog configuration pages.
- 9 Click **OK** to create the file volume.

You have now created a new volume. You must make this volume available to users before they can access it:

- For Windows NT users, create a share.
- For UNIX users, create an export.

Editing a File Volume

The Edit File Volume dialog box lets you:

- Rename the file volume
- Extend the size of an existing file volume
- Enable/disable quotas
- Change the trap threshold

You cannot change the volume group that the file volume is a part of.

An important aspect of managing file volumes is the concept of resizing file volumes. If a file volume becomes full of data, you can extend the file volume, thus alleviating the lack of space on the file volume.

To extend a file volume, there must be free storage space in the volume group that contains the file volume. This free space does *not* have to be on the same LUN as the file volume to be extended — you can create file volumes that span across arrays as long as the LUNs are in the same volume group. This gives you the option of extending existing file volumes by extending the volume group.

To edit an existing file volume:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **File Volumes**, then select **File Volumes Summary**.
- 3 Select the file volume you want to delete by clicking the row.
- 4 Select **Actions > Edit Selected File Volume**.
- 5 You can:
 - Enter a new name for the file volume.
 - Enter the size you want the file volume to become. Be careful to remain within the limits stated (current size must be greater than or equal to the new size, which must be less than or equal to the space available on the volume group).
 - Check or uncheck quota management enabled.
 - Change the SNMP trap threshold.
- 6 Click **OK**.

Deleting a File Volume

When you delete a file volume, the volume group reclaims the space it used.

Caution Deleting a file volume destroys all the data on that volume. This procedure cannot be reversed. Therefore, remove all crucial data before you delete the volume.

Before you proceed, make sure no one is accessing the file volume and delete all snapshots associated with the file volume.

To delete a file volume:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **File Volumes**, then select **File Volumes Summary**.
- 3 Select the file volume you want to delete by clicking the row.
- 4 Select **Actions > Delete Selected File Volume**.
- 5 Click **OK** to delete the file volume.

Managing Shares and Exports

Viewing Shares and Exports

Before network users can access the NAS server, you must give them permission. This is a security concern. Each platform grants permission differently:

- **Windows:** Shares are permissions that let you control Microsoft Windows users' access to data. You can create shares for any directory within a file volume, including the root. Once a share is created, users may attach to the share via the Network Neighborhood in Windows and store and retrieve files and directories. If you are operating under share-level security, you can limit access to shares by creating read-only or read/write passwords. See "HP NAS Server Security in an NT-only Environment" on page 30 for more information.
- **UNIX:** You create an export so that users can mount that volume/directory on their systems. However, you must first specify the access mode. If you specify a read-only or read/write access mode, users can use the `mount` command to access the volume from a UNIX workstation. This restriction is only for general access to the system. User-level restrictions also apply to all of the files and directories on the volume. See "HP NAS Server Security in a UNIX-only Environment" on page 29 for more information.

The Shares/Exports screen lets you:

- Create, edit, or delete SMB and NFS shares or exports
- Create, rename, or delete directories

You can also view either the Directories or Share Summary Table by selecting the icon in the toolbar or using the Actions menu.

Creating or Editing an SMB Share

You can control access to the NAS server data by creating SMB shares for Windows clients. A host allow list lets you limit which client machines are allowed access to the NAS server, regardless of the user.

To create or edit an SMB share:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **File Volumes**, then select **Shares/Exports**.
- 3 Select the file volume where you want to create the share by clicking the row.
- 4 Select **Actions > Create New SMB Share** (if you want to edit a share, select **Edit Selected SMB Share**).
- 5 Enter the **Share Name**.
- 6 Enter a **Share Comment**. The comment you enter here is optional and appears in the Network Neighborhood share properties comment field.
- 7 If you configured your system to use share-level security, enter a read-only password and a read/write password and confirm them.
- 8 If you wish, you can create a host allow list by clicking **Advanced** and following the steps below. If not, click **OK**.

To create a host allow list:

- 1 Click **Allow Selected Hosts**. The default is **Allow All Hosts** and this gives any machine access to the SMB share.
- 2 In the **Hostname/IP Address** field, enter the hostname or IP address of the machine you want to allow access from, then press **Enter**. Repeat this step for all machines that you would like to give access to. Wildcard (*) characters are accepted.
- 3 Click **OK**.

Creating or Editing an NFS Export

You can control access to the NAS server data by creating NFS exports for UNIX clients. A host allow list lets you limit which client machines are allowed access to the NAS server, regardless of the user.

To create or edit an NFS export:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **File Volumes**, then select **Shares/Exports**.
- 3 Select the file volume where you want to create the share/export by clicking the row.
- 4 Select **Actions > Create New NFS Export** (if you want to edit an export, select **Edit Selected NFS Export**).
- 5 Enter the **Mount Name**.
- 6 Select either **Read Only** or **Read/Write**.
- 7 If you wish, you can create a host allow list by clicking **Advanced** and following the steps below. If not, click **OK**.

To create a host allow list:

- 1 Click **Allow Selected Hosts**. The default is **Allow All Hosts** and this gives any machine access to the NFS export.
- 2 In the **Hostname/IP Address** field, enter the hostname or IP address of the machine you want to allow access from, then press **Enter**. Repeat this step for all machines that you would like to give access to. Wildcard (*) characters are accepted.
- 3 Click **OK**.

Deleting a Share or Export

To delete shares and exports:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **File Volumes**, then select **Shares/Exports**.
- 3 In the table, highlight the share/export you want to delete.
- 4 Select **Actions > Delete Selected SMB Share** or **Delete Selected NFS Export**.
- 5 Click **OK** to delete the share or export.

Verifying that the HP NAS Server Is Accessible to Users

Windows

To assign (map) a drive letter to a shared network resource, select **My Network Places** or **Network Neighborhood** (depending on your operating system) to map a drive to the shared resources (SMB shares) managed by the NAS server.

UNIX

Use the mount command to mount an exported network resource:

```
mount machine:/nfs/<NFS Mount Point Name>
```

where **<NFS Mount Point Name>** was the name defined by the administrator when the export was created.

Creating a Directory

You can create directories under the root level of a file volume, or under any directory in the hierarchy. Directories let you organize your data.

Note Before you can create a directory, you must already have created a file volume.

To create a directory:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **File Volumes**, then select **Shares/Exports**.
- 3 Navigate through the directory tree that appears in the browser and highlight the desired file volume or directory you want to create a new directory under.
- 4 Select **Actions > Create New Directory**.
- 5 Enter the directory name and click **OK**.

You have created a new directory. This directory is available to users only if the volume or directory in which it is located is already available. Otherwise, you must make this directory available to users before they can access it.

The new directory has a default permission setting (777 in UNIX, Everyone in Windows). After you use the Command View NAS to create a directory, you should modify the permissions (through a trusted host in UNIX, or in Windows Explorer) to suit your needs.

Renaming a Directory

To rename a directory:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **File Volumes**, then select **Shares/Exports**.
- 3 Navigate through the directory tree that appears in the browser and highlight the directory you want to rename.
- 4 Select **Actions > Rename Selected Directory**.
- 5 Enter a new name and click **OK**.

Deleting a Directory

You can delete directories to free up disk space or to remove unwanted data on the NAS server.

Caution Deleting a directory destroys all the data in that directory and all of its subdirectories. This procedure cannot be reversed. Therefore, remove all crucial data before you delete the directory.

To delete a directory:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **File Volumes**, then select **Shares/Exports**.
- 3 Navigate through the directory tree that appears in the browser and highlight the directory you want to delete.
- 4 Select **Actions > Delete Selected Directory**.
- 5 Click **OK** to delete the directory.

Replicating Data with Snapshots

Using Snapshots

A snapshot is a read-only picture of a file volume at a specific point in time. When you create a file volume, the snapshot of that file volume is of zero length. However, as you modify the file volume, the snapshot tracks changes between the original file volume and the modified file volume. If an error occurs and you want to revert to the previous version, you can use the snapshot data and the unmodified parts of the original file volume to quickly and easily construct the file volume.

When you set up a snapshot, consider how quickly the file's data will change, and how often you will delete snapshots and start over. You have the option to size snapshots relatively small and let them autogrow. As they reach the limit that you establish, their size can increase by approximately 10 percent to accommodate the changes. This flexibility lets you set the snapshot and not worry about a specific size.

After you specify a size, you must define an expiration date. When the snapshot expires, the system automatically deletes it. Consider your overall backup strategy in light of the snapshot expiration date. For example, you may want to take a snapshot of your data for a specified amount of time, then when you are certain that you have a backup of your system, delete the snapshot and begin the snapshot process again.

The system treats snapshots as part of a regular file volume. Snapshots appear in the **Snapshot Summary**. The Snapshot Summary screen displays:

- Snapshot name
- File volume the snapshot is a copy of
- Volume group the snapshot is a part of
- Space allocated to the snapshot
- Space used by the snapshot
- Space available for the snapshot
- Whether autogrow or notification is enabled and what the notification percentage is
- Expiration date of the snapshot
- Share count

You can identify a snapshot by the camera icon in the tree. You can create, edit, delete, and schedule snapshots.

Creating a Snapshot

You can use the snapshot feature to create a read-only point-in-time copy of a file volume.

To create a new snapshot:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Snapshots**, then select **Snapshot Summary**.
- 3 Select **Actions > Create New Snapshot**.
- 4 Select the file volume you want to take a snapshot of from the **File Volume** drop-down list.
- 5 Enter a **Snapshot Name**.
- 6 Enter the maximum size for the snapshot volume in the **Snapshot Capacity** field. A snapshot cannot exceed the file volume size.
- 7 In the Snapshot Capacity Policy box, select either:
 - **Auto Grow at** and select a percentage from the drop-down list to allow the snapshot to grow automatically if it is almost full.
Note: Remember, after the snapshot has been taken, when a file changes, the original file (at the time the snapshot is taken) is copied to the snapshot volume. So, for every file that changes, snapshot capacity is consumed. You want to specify a large enough capacity so that an original copy of all files that change is saved, but not so large that the snapshot volume takes up a lot of valuable storage space. You can always resize a snapshot at a later time.
 - **Send Notification at** and select a percentage from the drop-down list to send an SNMP alert when the space used on a snapshot volume reaches a certain percentage. When data is written to the new snapshot, the available space in the snapshot volume decreases.
Note: This percentage is used in conjunction with the settings you entered on the SNMP alert, email, and Syslog configuration pages.
- 8 In the Snapshot Expiration Policy box, select one of the following:
 - **Never** if you don't want this snapshot to be automatically deleted. If you select this option, you must delete the snapshot manually.
 - **On This Date** and specify a date and time for the snapshot to be deleted.
 - **After** and enter a day, week, or month value.
- 9 Click **OK** to create the snapshot and close the dialog box.

Editing a Snapshot

To edit a snapshot:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Snapshots**, then select **Snapshot Summary**.
- 3 Select the snapshot you want to rename.
- 4 Select **Actions > Edit Selected Snapshot**.
- 5 You can:
 - Enter a new **Snapshot Name**.
 - Enter the size you want the snapshot to become being careful to remain within the limits stated.
 - Change the snapshot capacity policy.
 - Change the expiration date.
- 6 Click **OK**.

Deleting a Snapshot

To delete a snapshot:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Snapshots**, then select **Snapshot Summary**.
- 3 Select the snapshot you want to delete.
- 4 Select **Actions > Delete Selected Snapshot**.
- 5 Click **Yes** to delete the snapshot.

Scheduling a Snapshot

On the Snapshots Scheduler page, a table displays the following information for each scheduled snapshot on the NAS server:

- File volume name of the snapshot
- Snapshot name
- Size allocated to the snapshot
- Auto grow enabled
- SNMP trap percentage
- Frequency of re-occurrence of the snapshot
- Expiration date of the snapshot

When you schedule a snapshot, make sure your NAS server will have sufficient space to accommodate the snapshot. (The system does not pre-allocate space and assumes that space will be available at the time the snapshot is scheduled to take place.) If space is not available on the volume group at the time the snapshot is scheduled to occur, the snapshot will fail. To ensure that you have sufficient space, you can view the Volume Groups page.

To create a scheduled snapshot:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Snapshots**, then select **Snapshot Scheduler**.
- 3 Select **Actions > Create New Scheduled Snapshot**.
- 4 Select the file volume you want to take a snapshot of from the **File Volume** drop-down list.
- 5 Enter a **Snapshot Name**.
- 6 Enter the maximum size for the snapshot volume in the **Snapshot Capacity** field. A snapshot cannot exceed the file volume size.
- 7 In the Snapshot Capacity Policy box, select either:
 - **Auto Grow at** and select a percentage from the drop-down list to allow the snapshot to grow automatically if it is almost full.

Note: Remember, after the snapshot has been taken, when a file changes, the original file (at the time the snapshot is taken) is copied to the snapshot volume. So, for every file that changes, snapshot capacity is consumed. You want to specify a large enough capacity so that an original copy of all files that change is saved, but not so large that the

snapshot volume takes up a lot of valuable storage space. You can always resize a snapshot at a later time.

- **Send Notification at** and select a percentage from the drop-down list to send an SNMP alert when the space used on a snapshot volume reaches a certain percentage. When data is written to the new snapshot, the available space in the snapshot volume decreases.

Note: This percentage is used in conjunction with the settings you entered on the SNMP alert, email, and Syslog configuration pages.

- 8 In the Snapshot Scheduler, select either **Once**, **Hourly**, **Daily**, **Weekly**, or **Monthly** and fill out the date and time information. When a snapshot is scheduled to occur more than once, the date and time of the occurrence is appended to the Snapshot Name that you specified. That way, older snapshots remain on the volume and are not overwritten.

- 9 In the Snapshot Expiration Policy box, select one of the following:

- **Never** if you don't want this snapshot to be automatically deleted. If you select this option, you must delete the snapshot manually.
- **On This Date** and enter a date and time for the snapshot to be deleted.
- **After** and enter a day, week, or month value.

- 10 Click **OK** to create the snapshot.

To delete the scheduled snapshot manually:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Snapshots**, then select **Snapshot Scheduler**.
- 3 Select the snapshot you want to delete.
- 4 Select **Actions > Delete Scheduled Snapshot**.
- 5 Click **OK** to delete the schedule snapshot.

Managing Quotas

Understanding Quotas

Quotas allow you to restrict the space usage on the NAS server for both users and groups. A user or group who goes beyond the specified space usage can not access the system. Each user can have one quota on a file volume.

Quotas are set on a per file volume basis. You can have a quota larger than the available space on the file volume.

Enabling or Disabling Quotas

To enable or disable a quota:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Quota Management**, then select either **User** or **Group Quotas**.
- 3 Select a file volume from the drop-down list.
- 4 Select **Actions > Enable/Disable Quotas**. If the file volume is:
 - Disabled, enabling it takes several minutes.
 - Enabled, disabling quotas applies to both users and groups.

Managing User Quotas

Configuring User Quotas

Note You must enable quota management on the file volume before you can create quotas.

This page lets you control the user quota settings.

To view user quotas that have been set on the NAS server:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Quota Management**, then select **User Quotas**.

A table displays the following information for every quota:

- User associated with the quota
- Space consumed by the user
- Space limit of the quota
- Grace space of the quota (Disk space that you can set as overflow space so that users can work beyond their space limits before cleaning up.)
- Email address of person to notify in case of space limitations

You can click on a column heading to sort items in that column. The **Actions** button lets you:

- Add a user quota
- Edit a user quota
- Delete a user quota
- Enable or disable quotas on the selected volume
- Import and export user quotas

You can also refresh the information in the table by clicking **Actions > Refresh**.

Adding a User Quota

To add a user quota:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Quota Management**, then select **User Quotas**.
- 3 Select an enabled file volume from the drop-down list.
- 4 Select **Actions > Add User Quota**.
- 5 Select a **Domain Name** and **User Name** from the drop-down lists.
- 6 Enter the:
 - **Space limit**: Space you want to allocate for this quota.
 - **Grace space**: “Cushion” of space in MB. By default, you have seven days to operate within the grace space. After seven days, you can not access the system until files and directories are cleaned up.
 - **Email address**: Person to notify when the quota space is reached.
- 7 Click **OK** to add the quota. Repeat steps 4 through 6 for any additional quotas you want to add.

Editing a User Quota

To edit a user quota:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Quota Management**, then select **User Quotas**.
- 3 Select an enabled file volume from the drop-down list.
- 4 Select the quota you want to edit by clicking the row.
- 5 Select **Actions > Edit User Quota**.
- 6 Change the:
 - **Space limit**: Space you want to allocate for this quota.
 - **Grace space**: “Cushion” of space in MB.
 - **Email address**: Person to notify when the quota space is reached.
- 7 Click **OK**.

Deleting a User Quota

To delete a user quota:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Quota Management**, then select **User Quotas**.
- 3 Select an enabled file volume from the drop-down list.
- 4 Select the quota you want to delete by clicking the row.
- 5 Select **Actions > Delete User Quota**.
- 6 Click **Yes** to delete the quota.

Note When you delete a user quota, the user has unlimited access to the storage.

Importing and Exporting User Quotas

You can apply user quotas via external files from this page. You can import quotas from a file into the NAS server or export the quotas in the NAS server to a file. All user list files and quota files are in text form to allow for easy editing and script conditioning.

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Quota Management**, then select **User Quotas**.
- 3 Select an enabled file volume, then select **Actions >** and one of the following options:
 - **Import User Quotas:** Imports user quotas into the system from an external file. File is read in and quotas are applied for every user in that file.
 - **Export User Quotas:** Exports all user quotas to a file. This file contains a line for every user in the system as well as their particular quotas.
 - **Export User List:** Exports a file that contains a list of users known to the system. This file helps in maintaining your external quota files.

Managing Group Quotas

Configuring Group Quotas

Note You must enable quota management on the file volume before you can create quotas.

This page lets you control the group quota settings.

To view group quotas that exist on your NAS server:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Quota Management**, then select **Group Quotas**.

A table displays the following information for every quota:

- Group associated with the quota
- Space consumed by the group
- Space limit of the quota
- Grace space of the quota (Disk space that you can set as overflow space so that groups can work beyond their space limits before cleaning up.)

You can click on a column heading to sort items in that column. The **Actions** button lets you:

- Add a group quota
- Edit a group quota
- Delete a group quota
- Enable or disable quotas on the selected volume
- Import and export group quotas

You can also refresh the information in the table by clicking **Actions > Refresh**.

Adding a Group Quota

To add a group quota:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Quota Management**, then select **Group Quotas**.
- 3 Select an enabled file volume from the drop-down list.
- 4 Select **Actions > Add Group Quota**.
- 5 Select a **Domain Name** and **Group Name** from the drop-down lists.
- 6 Enter the:
 - **Space limit:** Space you want to allocate for this quota.
 - **Grace space:** “Cushion” of space in MB. By default, you have seven days to operate within the grace space. After seven days, you can not access the system until files and directories are cleaned up.
 - **Email address:** Person to notify when the quota space is reached.
- 7 Click **OK** to add the quota. Repeat steps 4 through 6 for any additional quotas you want to add.

Editing a Group Quota

To edit a group quota:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Quota Management**, then select **Group Quotas**.
- 3 Select an enabled file volume from the drop-down list.
- 4 Select the quota you want to edit by clicking the row.
- 5 Select **Actions > Edit Group Quota**.
- 6 Change the:
 - **Space limit:** Space you want to allocate for this quota.
 - **Grace space:** “Cushion” of space in MB.
 - **Email address:** Person to notify when the quota space is reached.
- 7 Click **OK**.

Deleting a Group Quota

To delete a group quota:

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Quota Management**, then select **Group Quotas**.
- 3 Select an enabled file volume from the drop-down list.
- 4 Select the quota you want to delete by clicking the row.
- 5 Select **Actions > Delete Group Quota**.
- 6 Click **Yes** to delete the quota.

Note When you delete a group quota, the group has unlimited access to the storage.

Importing and Exporting Group Quotas

You can apply group quotas via external files from this page. You can import quotas from a file into the NAS server or export the quotas in the NAS server to a file. All group list files and quota files are in text form to allow for easy editing and script conditioning.

- 1 In the Command View NAS web interface, click the **Storage** tab.
- 2 Navigate down the tree to **Quota Management**, then select **Group Quotas**.
- 3 Select an enabled file volume, then select **Actions >** and one of the following options:
 - **Import Group Quotas:** Imports group quotas into the system from an external file. File is read in and quotas are applied for every group in that file.
 - **Export Group Quotas:** Exports all group quotas to a file. This file contains a line for every group in the system as well as their particular quotas.
 - **Export Group Lists:** Exports a file that contains a list of groups known to the system. This file helps in maintaining your external quota files.

Monitoring the System

6

In the Status tab, you can monitor the following information for the NAS server:

- Hardware event log
- System log
- Temperature status
- System voltage status
- Cooling fan status
- Memory status
- Power supply status
- UPS system status
- CPU utilization (current, peak, and average values)
- Network activity
- Client activity

You can view the overall environmental and activity status for all the major components including any attached storage arrays by selecting Status Summary.

High-Availability Status

If you have a high-availability NAS server, you can monitor:

- Nodes
- Failover packages

To view all high-availability log files, enter the following URL into a browser:

<http://<your-system-name>:280/halogs/>


A list of hyperlinked package control log files appears. Click on a file link to view the file.

Storage Array Status

If you want to monitor the storage array attached to your NAS server, a second browser window opens (Command View SDM) and lets you view the environmental and performance factors. The status tree displays either the array serial number or the alias name you gave the array.

Viewing the Status Summary

Status summary lets you view overall environmental and activity status for the NAS server, cluster components (if you have a high-availability NAS server), and any attached storage arrays. If an environmental item is running out of specification, a status symbol indicates the severity of the problem. The following symbols are used in the tables in this tab:

 : OK

 : An item is non-critical but warrants attention

 : An item is critical

 : The status information could not be obtained

 : Informational status only

You can click on an item in the table and select **Actions > View Details** to view the specific environmental area, or you can make your selections from the System Status tree.

To view the overall system status summary:

- 1 In the Command View NAS web interface, click the **Status** tab.
- 2 Navigate down the tree and select **Status Summary**.

The following status information appears for the NAS server:

- Temperature
- System voltages
- Cooling fans
- Memory
- Power supplies

The following status information appears for the cluster if you have a high-availability NAS server:

- Nodes
- Failover packages

At the top of the page, you can select a refresh rate (30 seconds to 5 minutes) for the displayed information.

If you have any attached storage arrays, you can view the environmental and performance status by clicking the array in the table and then selecting **Actions > Launch Command View SDM**.

Storage Array Status

Environment

You can view the overall environmental status for the attached array by launching the Command View SDM web interface. This interface opens in another browser window and gives you more detailed information about the array. The Command View SDM web interface lets you see more specific status information. For example, you can view a graphical representation of the array and its components. By clicking on the components, you can get further detailed information about the component and its status.

In the Status area on the Command View SDM, you also are able to review the total capacity of your array, including both allocated and unallocated storage.

Performance

You can view performance information on the array by launching the Command View SDM web interface. This interface opens in another browser window. You can obtain performance on any of 27 different performance metrics. You are able to select the specific performance parameters that you are interested in reviewing, add them to a graph, and view the information at an interval rate you select. Some of the performance parameters that you can review include:

- Read or write cache hits
- Read or write command latency
- Cache pages written or read
- Logical blocks written or read (per second)

Monitoring the NAS Server

Monitoring Events

Viewing the Hardware Event Log

The hardware event log collects information on the NAS server hardware (temperature, voltage, cooling fans, memory, power supplies) and generates a table listing the:

- #: The number of the event (most recent event listed first)
- **Status:** The state of the event
- **Code:** Additional information about the event and possible solutions
- **Event type:** Indicates the system or subsystem where the event occurred (such as, network card, SCSI card, processor, and so on)
- **Description:** A brief explanation of the event that occurred
- **Date/time:** The date and time the event was logged

The hardware event log can hold only 512 events. When the log reaches 256 events, a yellow alert message informs you that the log is filling up. When the log reaches 450 events, a red alert message prompts you to clear the log. If you do not clear the hardware event log, the log can not capture new events. The system does write every event to both the hardware event log and the system log.

If an event from the system event log causes the overall health of the NAS server to change, you must clear the hardware event log to reset the overall health status. The overall health status appears in the Command View NAS web interface's upper left corner.

To view the hardware event log:

- 1 In the Command View NAS web interface, click the **Status** tab.
- 2 Navigate down the tree to **Logs**, then select **Hardware Event Log**.

Using the drop-down list that appears at the beginning of the log, you can choose a refresh rate for the log. You can also select **Actions > Delete Event Log Entries**. When you clear the hardware event log, a warning advises you that the log's information will be permanently deleted. Because the System

Log also contains hardware event log messages and information about other system events, you can refer to this much larger log if necessary.

Viewing the System Log

You can view hardware and software system messages by displaying the system log.

To view the system log:

- 1 In the Command View NAS web interface, click the **Status** tab.
- 2 Navigate down the tree to **Logs**, then select **System Log**.

The following event information appears:

- **Severity:** The state of the system
- **Timestamp:** The date and time the event was logged
- **Program:** Name of the software module that generated the message
- **Description:** A brief explanation of the event that occurred

The system log is automatically cleared daily leaving only the 100 most recent messages in the log.

You can:

- Click on a column heading to sort items in that column. For example, you can sort by severity, timestamp, program, and description.
- Export a copy of the system log by selecting **Actions > Export System Log file**.
- Change the refresh rate for the displayed information by choosing a time interval from the drop-down list.

Monitoring the Environment

Viewing Temperature Status

This page gives the current temperature values in various locations:

- All CPUs
- System board
- Backplane

The screen displays temperatures in degrees Celsius. The status symbol indicates the state of the temperature.

A critical reading indicates that the temperature has gone outside the acceptable specified range. Make sure that all fans are properly installed and functioning.

Events that are listed on this page are also listed in the hardware event log and the system log.

To view the system temperatures:

- 1 In the Command View NAS web interface, click the **Status** tab.
- 2 Navigate down the tree to **Environment**, then select **Temperature**.

This page lets you:

- Change the refresh rate for the displayed information by choosing a time interval from the drop-down list.
- Click on a column heading to sort items in that column.

Viewing System Voltage Status

The system voltage status page provides information on the status of:

- System voltage
- Sensor location
- Current system voltage readings

Events that are listed on this page are also listed in the hardware event log and the system log.

To view the system voltage:

- 1 In the Command View NAS web interface, click the **Status** tab.
- 2 Navigate down the tree to **Environment**, then select **System Voltage**.

This page lets you:

- Change the refresh rate for the displayed information by choosing a time interval from the drop-down list.
- Click on a column heading to sort items in that column.

Viewing Cooling Fan Status

Cooling fans maintain the necessary ambient temperature for maximum performance of your NAS server. The NAS server has several processor and exhaust fans located in key hardware areas.

A table displays the RPMs of each fan along with the fan status.

If significant cooling fan problems are detected (a fan has stopped or is not spinning at a high enough rate), the event is posted to the hardware event log and the system log.

To view cooling fan status:

- 1 In the Command View NAS web interface, click the **Status** tab.
- 2 Navigate down the tree to **Environment**, then select **Cooling Fans**.

This page lets you:

- Change the refresh rate for the displayed information by choosing a time interval from the drop-down list.
- Click on a column heading to sort items in that column.

Monitoring Components

Viewing Memory Status

You can view the status of the memory modules installed in the NAS server. This page displays the total memory installed and the total number of memory slots on your NAS server.

To view the memory status:

- 1 In the Command View NAS web interface, click the **Status** tab.
- 2 Navigate down the tree to **Components**, then and select **Memory**.
- 3 A table displays the:
 - **Memory Slot:** The number of the memory slot
 - **Memory Size:** The size in MB of the memory module
 - **Memory Status:** The state of the memory

Events that are listed on this page are also listed in the hardware event log and the system log.

This page lets you:

- Change the refresh rate for the displayed information by choosing a time interval from the drop-down list.
- Click on a column heading to sort items in that column.

Viewing Power Supply Status

The NAS server monitors the installed power supplies. If a power supply sends an alert indicating that a failure is pending, the power supply status shows critical.

To monitor the status of the batteries in the NVRAM memory module in the attached storage array, you need to launch the Command View SDM web interface.

To view power supply status:

- 1 In the Command View NAS web interface, click the **Status** tab.
- 2 Navigate down the tree to **Components**, then select **Power Supplies**.

- 3 A table displays:
 - **Power Unit:** Number of the power supply
 - **Power Status:** State of the power supply
 - **Device Present:** Is the device present or not

This page lets you:

- Change the refresh rate for the displayed information by choosing a time interval from the drop-down list.
- Click on a column heading to sort items in that column.

A table listing the power supply events also displays on this page. To view further information about the event, click on the hyperlink code.

Events that are listed on this page are also listed in the hardware event log and the system log.

Note If a power supply is not installed, **Empty** displays in the table.

Viewing UPS Status

If you connected the optional UPS to your NAS server during installation, the NAS server attempts to communicate with the UPS through a serial connection. This page allows you to monitor the status of the UPS. If the UPS ever defaults to battery power, the system reports the status as an event, which is passed along to a management station as an SNMP trap.

To view UPS status:

- 1 In the Command View NAS web interface, click the **Status** tab.
- 2 Navigate down the tree to **Components**, then select **UPS**.
- 3 A table displays:
 - **UPS Status:** State of the UPS
 - **UPS Message:** Is the device present or not

This page lets you:

- Change the refresh rate for the displayed information by choosing a time interval from the drop-down list.
- Click on a column heading to sort items in that column.

Monitoring Performance

Viewing CPU Utilization

CPU utilization lets you view the current, peak, and average load on all the installed CPUs in your NAS server.

To view the CPU Utilization:

- 1 In the Command View NAS web interface, click the **Status** tab.
- 2 Navigate down the tree to **Performance**, then select **CPU Utilization**.
- 3 A table displays:
 - CPU Number
 - Current CPU utilization
 - Peak CPU utilization
 - Average CPU utilization

This page lets you:

- Change the refresh rate for the displayed information by choosing a time interval from the drop-down list.
- Click on a column heading to sort items in that column.

Viewing Network Activity

You can view network transmission information to see how much data is flowing across the network NIC ports in the NAS server. You can use this information to ensure that your network is running as efficiently as possible. If one of the NIC ports has too much traffic, you may want to move clients to another available NIC port. You can also view errors and collisions to spot potential hardware problems.

To view network activity:

- 1 In the Command View NAS web interface, click the **Status** tab.
- 2 Navigate down the tree to **Performance**, then select **Network Activity**.
- 3 A table displays the network activity of the:
 - NIC Port number
 - MAC Address
 - IP Address

- Packets Received
- Receive Errors
- Packets Transmitted
- Transmit Collisions

This page lets you:

- Change the refresh rate for the displayed information by choosing a time interval from the drop-down list.
- Click on a column heading to sort items in that column.

Viewing Client Activity

You can view information about the clients that are currently attached to the NAS server.

To view client activity:

- 1 In the Command View NAS web interface, click the **Status** tab.
- 2 Navigate down the tree to **Performance**, then select **Client Activity**.
- 3 A table displays the network activity of the:
 - **Protocol**: Type of connection (for example, Telnet, NFS, console, and so on)
 - **Client Name**: IP address or the system name
 - **Volume**: Where the user is attached
 - **Path**: Location of the volume
 - **Connected At**: Date and time the user logged on
 - **Comment**: Information about the connection such as the user identity

This page lets you:

- Change the refresh rate for the displayed information by choosing a time interval from the drop-down list.
- Click on a column heading to sort items in that column.

Monitoring High-Availability Settings

Monitoring Nodes

Note This section applies only if you have purchased a high-availability NAS solution.

This screen lets you monitor the status of the two nodes (servers) in your cluster.

To monitor the nodes:

- 1 In the Command View NAS web interface, click the **Status** tab.
- 2 Navigate down the tree to **High Availability**, then select **Nodes**.
- 3 A table displays:
 - Node name
 - Status of the node

Using the drop-down list that appears at the beginning of the log, you can choose a refresh rate for the log.

Monitoring Failover Packages

Note This section applies only if you have purchased a high-availability NAS solution.

This screen lets you monitor the status of the failover packages in your cluster.

To monitor the failover packages:

- 1 In the Command View NAS web interface, click the **Status** tab.
- 2 Navigate down the tree to **High Availability**, then select **Failover Packages**.
- 3 A table displays:
 - Name of the package
 - Status of the package

Using the drop-down list that appears at the beginning of the log, you can choose a refresh rate for the log.

Enabling Virus and Backup Software



HP Virus Guard, HP OpenView OmniBack, and snapshots are optional software components that are preloaded on the NAS server. They must be enabled before they can be used.

- 1 In the Command View NAS web interface click the **Applications** tab.
- 2 Select either **Anti-Virus**, **hp omniback**, or **Snapshots**.
- 3 In the resulting screen, the Status field indicates whether the software is enabled. By default, Anti-Virus and OmniBack are disabled; snapshots is enabled. If **Disabled** appears, select **Actions > Enable/Disable Application**.

Using NAS Virus Protection

Overview

The anti-virus software, HP Virus Guard, works to prevent computer viruses from contaminating data stored on the NAS server and therefore prevents the device from being a “transmitter” of viruses across the network.

The anti-virus software uses two methods for protecting the system from becoming contaminated by a computer virus:

- **Scan Control:** Scans the storage device on a regular basis, searching stored data for identifying strings or “signatures” that indicate the presence of a virus. While this method can effectively identify viruses once they are on the system, there can be a significant time lag between the time the virus is copied onto the system and the time the virus is detected.
- **Real Time Protection (RTP):** Monitors all data being written to the storage device and checks the data for computer viruses.

The software provides the following capabilities:

- Virus handling options including clean, rename, quarantine, log, and delete
- Immediate detection and handling of viruses as they are copied to the NAS server (real time protection)
- Artificial intelligence mechanism, heuristic scanning, to detect unknown viruses
- Virus signature updates directly from the scan engine vendor
- Scan and RTP logging which includes number of files scanned, viruses found, and response taken
- Automatic scheduling for both virus scanning and signature file updates
- Notification of detected viruses by email

You can access the HP Virus Guard web interface from the **Applications** tab.

- 1 In the Command View NAS web interface click the **Applications** tab.
- 2 You must enable HP Virus Guard before launching the software. Select **Anti-Virus**. In the resulting screen, the **Status** field indicates whether the software is enabled (disabled is the default state). If **Disabled** appears, select **Actions > Enable/Disable Application**.
- 3 Select **Actions > Manage/Configure Application**. The HP Virus Guard web interface appears.

The HP Virus Guard interface displays the:

- **HP Virus Guard version:** Version number of HP Virus Guard you have installed on your system.
- **Virus definition file version:** List of all viruses updated as well as the date and version number.
- **Real time protection status:** Whether this feature is enabled or disabled.
- **Expiration date:** Date the software expires (one year after purchase). After the expiration, you can purchase another year of HP Virus Guard.

The HP Virus Guard web interface lets you:

- Update virus files
- Schedule a scan
- Control real time protection
- Manage quarantined files
- View logs

If you have a high-availability NAS server, you can configure HP Virus Guard through any node in the cluster (tasks are synchronized between boxes automatically). Real time protection and scan tasks can have both local and non-local storage configured in one task.

Updating the Virus File

The HP Virus Guard web interface lets you download the latest version of the HP Virus Guard engine and signature file and schedule updates as they become available.

In the HP Virus Guard web interface, select **Virus File Updates**.

Enter the local proxy server and port information, then click **Apply** to save these settings. The **Download Site** field contains the default location. If you change this default location and later want to restore it, click **Defaults**.

Use the **Actions** button to update the virus file or schedule an update.

This screen lists the:

- Current HP Virus Guard version
- Signature version
- Update schedule

To update the virus file:

- 1 Select **Actions > Update Now**.
- 2 A dialog box appears showing the status of the update.

To schedule an update:

- 1 Select **Actions > Schedule Updates**.
- 2 The schedule update screen appears. Select either:
 - **Disable** so you can unschedule updates from running automatically
 - **Run Once** and select the date and time information
 - **Run Every** and select the date and time information

Using Scheduled Scan Control

Understanding Scheduled Scan Control

Scheduled scan control lets you schedule a scan for viruses on your volumes and decide what action to take when a virus is detected.

From the HP Virus Guard web interface, select **Scheduled Scan Control**.

A table displays the following information for every scan:

- Scan task name
- Next scheduled run time
- Frequency of the scan
- Whether snapshots of the volume are scanned
- Actions for the scan
- Volumes to be scanned

You can click on a column heading to sort items in that column.

The scan control screen lets you:

- Create a new scan task
- Perform a scan now
- View scan task status
- Edit a scan task
- Delete a scan task
- Copy a scan task

Creating and Editing a Scan Task

To create a new scan:

- 1 In the HP Virus Guard web interface, select **Scheduled Scan Control**.
- 2 Select **Actions > Create New Scan Task**.
- 3 Enter a name for the scan task.
- 4 In the Detection tab:
 - Select the volume to be scanned from the Available Volumes list, then click **Add**. You can add more than one volume.

- b** Select whether you want to scan **All Files** or **Program Files only**.
Selecting **Program Files only** scans files based on a list of extensions that are commonly susceptible to viruses on Windows systems and scans all files with x-bit on UNIX systems.
 - c** Check whether you want to scan **Compressed Files**. These include:
 - ARJ
 - GZIP
 - JAVA archive
 - LHA
 - Microsoft cabinet file
 - Microsoft compressed file
 - MIME
 - UNIX to UNIX encoded files (UUEncode)
 - ZIP
 - RAR
 - UNIX compressed file (.Z)
 - Rich Text Format file (.RTF)
 - d** Check whether you want to virus-scan all **Snapshots** that exist for the volumes you selected. Snapshots are read-only so if the scan finds a virus, it is only recorded in the log.
 - e** Check whether you want to **Enable Heuristic Scanning**. This lets you find new virus strains by detecting virus-like characteristics. Selecting this option will slow down your scan.
- 5** Click the **Schedule** tab, select either:
 - a** **Disable** so you can unschedule the scan task without deleting it. You can still select **Actions > Scan Now** to run the task.
 - b** **Run Once** and select the date and time information
 - c** **Run Every** and select the date and time information
- 6** Select the **Actions** tab and select what action you want the software to take when a virus is found:
 - a** Log only
 - b** Quarantine

- c Rename
 - d Delete
 - e Clean (attempts to clean the virus)
 - f Clean, quarantine if unable to clean
 - g Clean, rename if unable to clean
- 7 Click the **Alerts** tab. If you want to be notified when a virus is found, either enter an email address or check **Send virus alerts using SNMP**. To receive email alerts, you must enter information in the SNMP or Email alert settings pages in the Command View NAS web interface.
 - 8 Click **OK** to create the scan task.
- To edit a scan task:
- 1 From the HP Virus Guard web interface, select **Scheduled Scan Control**.
 - 2 Select the scan task you want to edit by clicking the row.
 - 3 Select **Actions > Edit Scan Task**.
 - 4 Select any of the tabs in the dialog box and make any modifications necessary.

Performing a Scan Task and Viewing the Status

To perform a scan task:

- 1 In the HP Virus Guard web interface, select **Scheduled Scan Control**.
- 2 Select the scan task you want to scan by clicking the row.
- 3 Select **Actions > Scan Now**. (**Note:** If you have a high-availability NAS server, this option does not appear. You can only run scheduled scan tasks.)
- 4 A dialog box appears displaying:
 - Name of the scan task
 - Action of the scan task (log, etc.)
 - Number of files scanned
 - Number of viruses found
- 5 You can click **Stop** to terminate the scan task or **OK** to close the dialog box.

To view the status of a running scan task:

- 1 In the HP Virus Guard web interface, select **Scheduled Scan Control**.
- 2 Select the scan task you want to view the status of by clicking the row.
- 3 Select **Actions > View Scan Task Status**.
- 4 A dialog box appears displaying:
 - Name of the scan task
 - Action of the scan task (log, etc.)
 - Number of files scanned
 - Number of viruses found
- 5 You can click **Stop** to terminate the scan task or **OK** to close the dialog box.

Copying a Scan Task

Copying a scan task is an easy way to duplicate a scan's detection settings, schedule, actions, and alerts if you want to use the same settings on another scan. You need to change the volumes for the copied scan task and adjust any settings as necessary.

To copy a scan task:

- 1 In the HP Virus Guard web interface, select **Scheduled Scan Control**.
- 2 Select the scan task you want to copy by clicking the row.
- 3 Select **Actions > Copy Scan Task**.
- 4 Enter a new task name in the **Copy to** field.

Deleting a Scan Task

To delete a scan task:

- 1 In the HP Virus Guard web interface, select **Scheduled Scan Control**.
- 2 Select the scan task you want to delete by clicking the row.
- 3 Select **Actions > Delete Scan Task**.

Using Real Time Protection Control

Understanding Real Time Protection Control

Real Time Protection (RTP) scans each file in the selected volume immediately after the volume is written to the storage system, thereby protecting the NAS server from viruses that could spread across the network. RTP can hinder your device's performance, depending on the amount of files that are changed on the protected volume.

From the HP Virus Guard web interface, select **Real Time Protection Control**.

A table displays the following drive information for every scan:

- RTP task name
- Actions for the scan
- Volumes to be scanned

You can click on a column heading to sort items in that column.

The real time protection screen lets you:

- Create a new RTP task
- Edit an RTP task
- Change your RTP global settings
- Delete an RTP task

Creating and Editing an RTP Task

To create a new RTP task:

- 1 In the HP Virus Guard web interface, select **Real Time Protection**.
- 2 Select **Actions > Create New RTP Task**.
- 3 Enter a name for the real time protection task.
- 4 In the **Detection** tab, select the volumes to be scanned from the Available Volumes list, then click **Add**.
- 5 Click the **Actions** tab and select what action you want the software to take when a virus is found:
 - Log only
 - Quarantine
 - Rename

- Delete
 - Clean (attempts to clean the virus)
 - Clean, quarantine if unable to clean
 - Clean, rename if unable to clean
- 6 Click the **Alerts** tab. If you want to be notified when a virus is found, either enter an email address or check **Send virus alerts using SNMP**. To receive email alerts, you must enter information in the SNMP or Email alert settings pages in the Command View NAS web interface.
 - 7 Click **OK** to create the scan task.

To edit an RTP task:

- 1 In the HP Virus Guard web interface, select **Real Time Protection**.
- 2 Select the RTP task you want to edit by clicking the row.
- 3 Select **Actions > Edit RTP Task**.
- 4 Select any of the tabs in the dialog box and make any modifications necessary.

Changing RTP Global Settings

To change the global settings for all RTP tasks:

- 1 In the HP Virus Guard web interface, select **Real Time Protection**.
- 2 Select **Actions > RTP Global Settings**.
- 3 A dialog box appears displaying your RTP global settings.
 - a Select either **All files** to scan all files in the volume or **Program files** to scan files based on a list of extensions that are commonly susceptible to viruses on Windows systems and all files with x-bit on UNIX systems.
 - b Select **Scan compressed files** if you want to scan files such as:
 - ARJ
 - GZIP
 - JAVA archive
 - LHA
 - Microsoft cabinet file
 - Microsoft compressed file
 - MIME

- UNIX to UNIX encoded files (UUEncode)
- ZIP
- RAR
- UNIX compressed file (.Z)
- Rich Text Format file (.RTF)
- c Select **Enable Heuristic Scanning** if you want to find new virus strains by detecting virus-like characteristics. Selecting this option will slow down your scan.

Deleting an RTP Task

To delete an RTP task:

- 1 In the HP Virus Guard web interface, select **Real Time Protection**.
- 2 Select the scan task you want to delete by clicking the row.
- 3 Select **Actions > Delete RTP Task**.

Managing Quarantined Files

When you set up a scan or RTP task, you can choose from a variety of different actions for the software to take if it detects a virus. If you select to quarantine a virus, the software will quarantine any viruses it finds, and you can manage these virus files in the Manage Quarantined Files section.

A table displays the following information:

- Full path to the quarantined file's original location
- Virus name
- Date the file was last modified

You can:

- Delete or retrieve a file from quarantine
- Delete or retrieve all of the quarantined files

Caution When you retrieve a file, the software places the virus file back to its original location on the NAS device. Real Time Protection suspends temporarily while the file is retrieved.

If you perform one of the following tasks, you must make sure that the directory exists:

- Start an RTP task with quarantine
- Create virus files in multiple directories
- Verify that files are in quarantine bucket
- Remove the directory in which the virus file resided
- Retrieve files

If the directory has been moved or deleted, the files are not retrieved.

To delete or retrieve a file:

- 1 In the HP Virus Guard web interface, select **Manage Quarantined Files**.
- 2 Select:
 - **Actions > Delete File** to permanently delete the file from quarantine
 - **Actions > Retrieve File** to restore the file to its original location (the directory must exist)

To delete or retrieve all the files in the table:

- 1 In the HP Virus Guard web interface, select **Manage Quarantined Files**.
- 2 Select:
 - **Actions > Delete All** to permanently delete all the files in the table
 - **Actions > Retrieve All** to restore all quarantined files to their original location (the directory must exist)

Viewing Virus Logs

In the HP Virus Guard web interface, select **Logs**.

This screen displays the following information for your virus logs:

- Date and time of the scan
- Scan task name
- Log type (can be one of the following):
 - RTP — Each day where an RTP and has scanned a file has an entry
 - Scan— Each task that is run has an entry
 - Update — Each update that occurs has an entry
- Status of the scan
- Number of files scanned
- Number of viruses found

The **Actions** buttons lets you view details on a particular log, delete a log, or delete all of the logs. You can click on a column heading to sort items in that column.

To view a log:

- 1 Select the log you want to view details on by clicking the row.
- 2 Select **Actions > View Log**.
- 3 The View Log dialog box appears detailing the information on the task.

To delete a log:

- 1 Select the log you want to delete on by clicking the row.
- 2 Select **Actions > Delete Log**.

To delete all logs, select **Actions > Delete All Logs**.

Using the Backup Agent

The NAS server has many built-in features that help you protect your data, such as RAID storage, active spares, and redundant power supplies. However, in the event of disaster, it is important that you have a data recovery plan that includes snapshots (creates a read-only, point-in-time, copy of a volume), regular backups, and maintaining copies of the system's configuration using the disaster recovery feature.

The two methods of backing up the data on your NAS server are:

- **Basic Network Backup:** Network backup uses separately purchased backup software and a tape device to protect network visible files. See “Integrating with Network Backup Applications” on page 159 for the more information about the applications that integrate with the NAS server.
- **Backup with NAS Agent:** The HP Omniback II 4.1 backup agent pre-loaded on the NAS server provides enhanced backup capabilities. The backup agent receives commands from and is controlled by the Omniback II Manager application.

The backup agent must be enabled via the Command View NAS web interface to be fully functional. To use a tape library, you may need additional licenses, depending on your OmniBack version and configuration (see <http://www.openview.hp.com/products/omniback/> for details).

With the backup agent on the NAS server, the backup/restore operations are independent of network file protocols (CIFS or NFS), and any OmniBack II backup server can preserve the full set of file attributes. The performance of file access is also improved.

With a locally attached tape device, the backup operations do not transfer file data over the network.

Connecting Tape Devices

If you purchased a tape library with your NAS server, your server has either two single-port SCSI cards installed or one to two FC cards for tape connections. The HP NAS 8000 supports the HP tape and tape library products. For updated information about supported tape devices, please refer to the HP NAS 8000 support web page (<http://www.hp.com/support/nas8000>).

See the installation guide that came with the tape device for more information, or the Tape Library Upgrade section in this user's guide.

Using HP OpenView OmniBack II and the NAS Backup Agent

HP OpenView OmniBack II is a backup solution that provides reliable data protection and high accessibility for your data. OmniBack II offers comprehensive backup and restore functionality specifically tailored for enterprise-wide and distributed environments.

You can use OmniBack II version 4.0 or 4.1 on either a Windows NT or UNIX system connected to your NAS server. Each tape drive requires an Omniback II drive extension license. If all of the tape UNIX drive extension licenses are assigned for your installation, additional UNIX drive extension licenses will be required to add tape drives connected to the HP NAS 8000. For details about OmniBack II licenses see the *Omniback II Installation and Licensing Guide*.

Enabling the NAS 8000 Backup Agent

The NAS 8000 backup agent is preinstalled and authorized, but you must enable it.

- 1 In the Command View NAS web interface, click the **Applications** tab.
- 2 Navigate down the Applications tree and select **hp omniback**.
- 3 Select **Actions > Enable/Disable Application**.
- 4 Click **Yes** to enable to application.

You are now ready to back up files. Control of the backup processes and the backup devices is provided in the OmniBack II Manager's interface. You can use the interface to:

- Import and configure the client (the NAS 8000)
- Configure the tape devices connected to the NAS 8000
- Configure the backup specifications
- Run your backup and restore operations

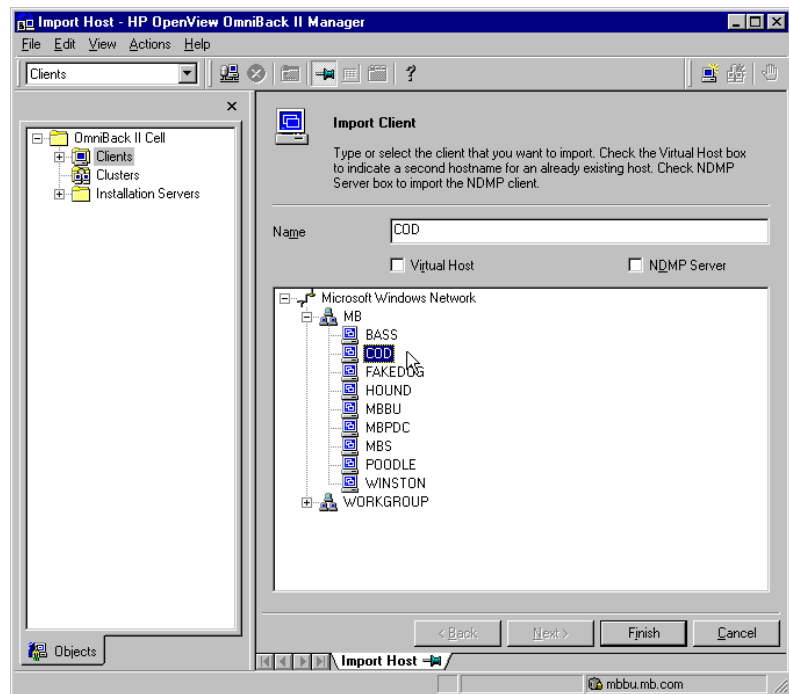
These procedures are described in detail in the *HP OpenView OmniBack II Installation and Licensing Guide* and the *HP OpenView OmniBack II Administrator's Guide*. You can return to the Command View NAS web interface to select snapshot behavior during backup or to set OmniBack II agent parameters in the .omnirc file that could be necessary in special cases.

Importing the Client to an OmniBack II Cell

- 1 Select **Start > HP OmniBack II > OmniBack II Manager**.
- 2 Verify that **Clients** is selected in the drop-down list in the top left corner of the window.
- 3 Select **Clients** from the tree and right-click. Select **Import Client**. If the NAS 8000 agent needs to be deleted from the OmniBack II Manager, delete the NAS 8000 client and click **No** when asked if the software should be removed.

Note: You can not delete the OmniBack II agent software from the NAS 8000 system.

Figure 1 OmniBack Client



- 4 Expand the network and find the NAS server (on HP-UX, enter the node name). Select it and click **Finish**. The NAS server now appears in the Clients list. This associates the OmniBack II software with the client

software on the NAS server. For details how to import an OmniBack II client into a cell, see the *HP OpenView OmniBack II Installation and Licensing Guide*.

Configuring a Backup Device

- 1 Select **Devices & Media** from the drop-down list, then select **Devices** from the tree. Right click, and select **Add Device or Autoconfigure Devices**.
- 2 Type a **Device Name** and **Description** and change the **Device Type** to **SCSI II Library**. Click **Next**.
- 3 In the **SCSI address of filename of the Library robotic** drop-down list, select the tape library and click **Next**.
- 4 The next screen displays available slots when connected to a HP Tape Library. Click **Add**, then click **Next**.
- 5 Select the media type for the tape library from the drop-down list, then click **Finish**.
- 6 You have now successfully configured the library. Click **Yes** to configure the drives.

Configuring the Tape Drives

- 1 In the dialog that appears, type a **Device Name** and **Description**, then click **Next**.
- 2 Look to see what **Drive Index** is noted in the field. Select the **SCSI Address or filename of Data Drives** from the drop-down list that matches the Drive Index. Repeat this step for all the drives.
- 3 Select the appropriate mediapool.
- 4 Click **Finish**.

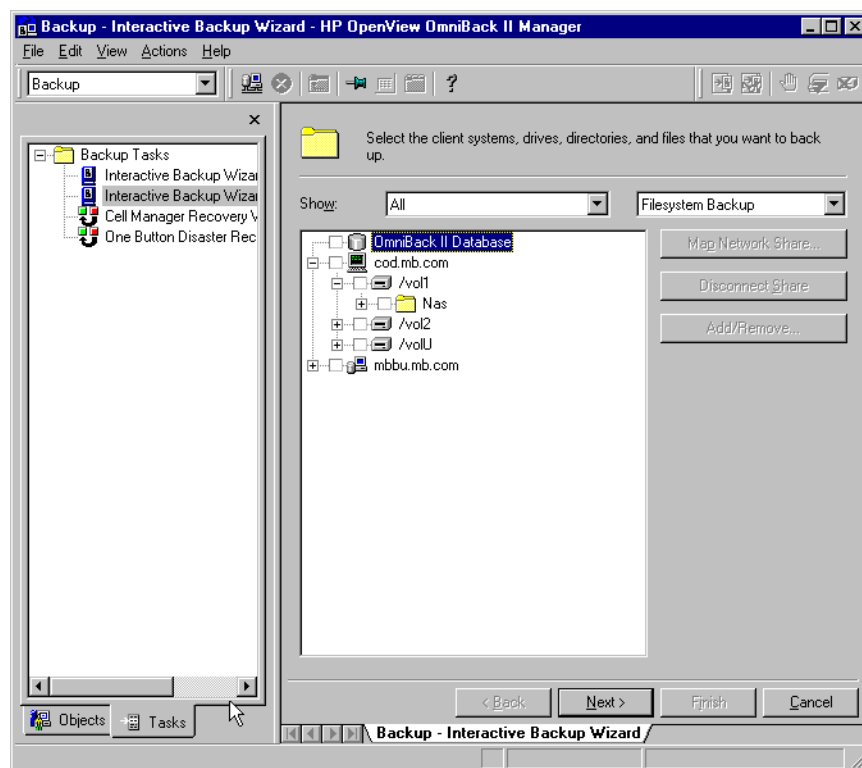
For details how to configure backup devices within OmniBack II, see the *HP OpenView OmniBack II Administrator's Guide*.

Backing Up Files

To back up files from the NAS server using OmniBack II:

- 1 Verify that **Backup** is selected in the drop-down list in the top left corner of the window.
- 2 Click the **Tasks** tab on the bottom of the screen, then click **Interactive Backup Wizard**.

Figure 2 Interactive Backup Wizard



- 3 Verify that **Filesystem Backup** is selected in the drop-down list.
- 4 Select your the node you will back up. You can only back up nodes running the OmniBack II agent.
- 5 Select the files, directories, or volumes you want to back up.

- 6 Select your backup options as you normally would, then start the backup.
- 7 Select the tape devices to backup to, this can include NAS server attached tape devices.

For more information about using OmniBack II, see the OmniBack II documentation.

Managing and Configuring the HP OpenView OmniBack II NAS Agent

You can use the Command View NAS web interface for selecting snapshot behavior during backup or for setting agent parameters that could be necessary in special cases.

- 1 In the Command View NAS web interface, click the **Applications** tab.
- 2 Navigate down the tree and select **OmniBack Backup**.
- 3 Select **Actions > Manage/Configure Application**. The following window appears:

Figure 3 Managing OmniBack II

The screenshot shows a web browser window with the address bar displaying `http://fakedog:280/cgi-bin/addons/backupOB/omniConfig.sh`. The page title is "Managing OmniBack II Agent". Below the title, there is a "Troubleshooting" button and a "? Help" button. The main configuration area contains the following fields and buttons:

- Backup Snapshot Behavior:** A dropdown menu currently showing "Backup without Snapshot".
- Backup Snapshot Volume Percentage (10 - 100):** A text input field containing the value "10".
- Save** button.
- OmniBack II Port Number:** A text input field containing the value "5555".
- Save** button.
- Refresh** and **Close Window** buttons at the bottom.

The table below explains each of this window's fields:

Field	Description
Backup Snapshot Behavior	<p>Drop-down list that controls the behavior of snapshots for the backup session. There are three selections for this field:</p> <ul style="list-style-type: none">■ Utilize a snapshot when performing the backup. If this selection is chosen, make sure that the snapshot volume percentage field is large enough to accommodate the snapshot for the backup.■ Perform the backup utilizing the snapshot mechanism, but if the snapshot fails, the backup will continue. <p>Perform the backup without utilizing snapshots (default).</p>
Backup Snapshot Volume Percentage	<p>Defines the size of the snapshot in terms of the percentage of the original volume's space. Set the value between 10 and 100 percent (10 - 100).</p>
OmniBack II Port Number	<p>The default port number is 5555, when this value is changed the agent will be restarted. Do not change during a backup.</p>

Snapshot Behavior: Per-volume Snapshot Backup

The HP NAS operating system lets you take a snapshot (checkpoint) of an entire volume so that you can create a point-in-time copy of all files. OmniBack II agent for HP NAS helps you create a snapshot before backup, then backs up the files from this snapshot volume. After you perform a backup, the snapshot is removed.

Note that OmniBack II agent creates an individual snapshot for each volume just before a backup. Therefore, a point-in-time copy applies only to a single volume. If your application stores data in two or more volumes, the snapshot backup will not provide a consistent point-in-time copy of the files.

By default, the size of a snapshot volume is 10 percent of the original volume's size. The snapshot volume size must be large enough to accommodate all of the changed files during the backup task. If a snapshot exists for a long time and many changes occur on the original file system during this time, the snapshot volume can become full. Therefore, OmniBack II provides a variable you can use to set the size of a snapshot volume. This variable (OB2HPNASSNAPSHOTSIZE) resides in the .omnirc file. The Command View NAS web interface provides an interface in which you can set this variable.

You should set the size of the snapshot so that the snapshot volume does not become full during backup. If the snapshot volume becomes full, the snapshot volume is no longer valid and the backup is therefore aborted.

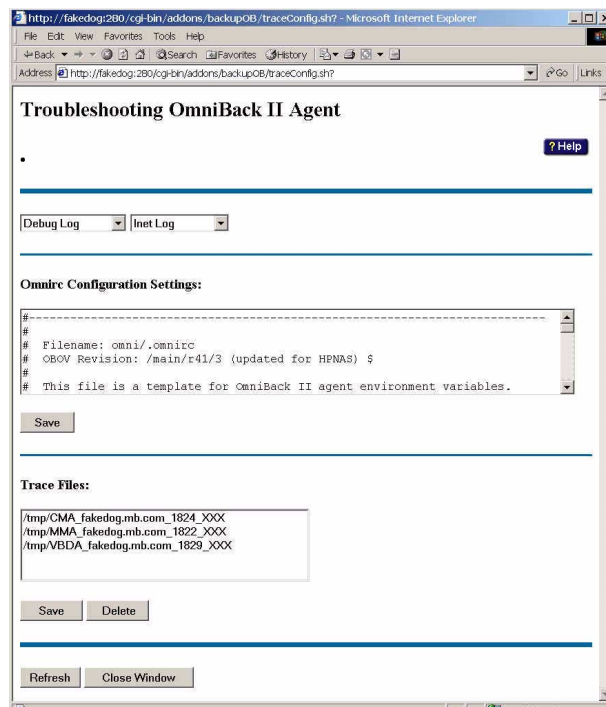
By default, OmniBack II aborts the backup if the snapshot cannot be created. You can use the OB2HPNASSNAPSHOT option to change this behavior. The following values are available:

- 0: default behavior (includes snapshot)
- 1: continue backup of normal volume if snapshot cannot be created
- 2: do not try to create a snapshot

Troubleshooting the OmniBack Agent

When you click **Troubleshooting** in the Managing OmniBack II Agent window, the following appears:

Figure 4 Troubleshooting OmniBack II Agent



The table below explains each of this window's fields.

Field	Description
Debug Log	<p>Drop-down list that allows access to the Debug Log. The Debug Log is always enabled. There are two selections for this field:</p> <ul style="list-style-type: none">■ View: Save the file to local storage.■ Clear: Clear the contents of the Debug Log.
Inet Log	<p>Drop-down list that allows control of the Inet Log and the Inet Trace Files. There are three selections for this field:</p> <ul style="list-style-type: none">■ View: Views the Inet Log and lets you save the file to local storage.■ Clear: Clear the contents of the Inet Log.■ Start or Stop Inet Trace File generation: The Inet Trace Files can be viewed or deleted using the Trace File window below.
Omnirc Configuration Settings	<p>This edit box displays the contents of the .omnirc file. This file should only be changed as directed by HP Omniback support for special configurations.</p> <p>Save: Writes the administrator's changes to the NAS 8000 .omnirc file.</p>
Trace Files	<p>Selection box that allows access to the Trace Files. The Trace Files are enabled from the OmniBack II Manager. There are two selections for this field:</p> <ul style="list-style-type: none">■ Save: The file is transferred to the local system and can be saved to disk. These files can be large and can take time for the transfer to occur. <p>Delete: The selected file is deleted.</p>

Restrictions specific to the NAS 8000:

- OmniBack II object pre/post exec scripts cannot be configured on the NAS server.
- User-defined volume names must not contain characters that are not allowed for UNIX directory names.
- The prerequisite for restoration to the original location is that the volume (with its user-defined volume name that was used for backup) exist and is configured on the system.
- Although files backed up on NAS 8000 can be restored to alternative locations (like files backed up on any other OBII client), the Windows

security attributes will not be restored on the alternate location. Windows and UNIX restorations also behave in this manner.

- When managing OmniBack II clients, the OmniBack agent software for the NAS server cannot be added, nor can the agent software be removed. The OmniBack agent for the NAS server is an integrated part of the NAS server.
- The NAS server cluster configuration is not supported in the OmniBack II cluster capabilities. Backup of the NAS cluster nodes require manual configuration and possible reconfiguration following failover of NAS nodes.
- Disaster recovery for the NAS server is not automated by OmniBack II, but the disaster-recovery file can be saved to tape using OmniBack II. Refer to Recovering from a Disaster.

For updated configuration and troubleshooting information, refer to the NAS 8000 support web site (<http://www.hp.com/support/nas8000>).

Enabling Snapshots

You can use the snapshot feature to create a read-only point-in-time copy of a file volume.

- 1 In the Command View NAS web interface click the **Applications** tab.
- 2 You must enable Snapshots before launching the software. Select **Snapshots**. In the resulting screen, the **Status** field indicates whether the software is enabled. If **Disabled** appears, select **Actions > Enable/Disable Application**.
- 3 Select **Actions > Manage/Configure Application**. In the resulting Snapshots window (on the Storage tab), you can access the following capabilities:
 - Creating a Snapshot
 - Editing a Snapshot
 - Deleting a Snapshot
 - Scheduling a Snapshot

See “Using Snapshots” on page 100 for more information.

Recovering from a Disaster

8

If the NAS server or storage array sustains hardware failures, you can use the NAS device's disaster-recovery capability to restore your system configuration and storage settings to a previously saved state.

The disaster recovery feature is automatically enabled when you install the NAS operating system. A disaster recovery file (DRF) is built from the system configuration data and is generated every 30 minutes. A backup copy of the existing DRF is made prior to the generation of each new DRF.

The DRF contains all the information necessary to rebuild the NAS server and storage array configuration from the point in time when the system created the DRF. This information includes:

- The NAS registry
- System configuration files, as referenced in the NAS registry
- System logs, as referenced in the NAS registry
- Storage settings (for example, LUNs and LUN sizes, volume groups, volumes, shares)

The DRF is stored in a local system volume on the NAS server named "DISASTER_RECOVERY." You should regularly store a backup of this volume on tape, or copy it to another system using NFS or CIFS. **You must back up the DISASTER_RECOVERY volume or you cannot use the NAS 8000 disaster recovery features. In the event of a disaster, the DRF is required as part of the general recovery process.**

To make the DISASTER_RECOVERY volume shareable to other systems, execute the following text commands:

```
AddStorageShare DISASTER_RECOVERY /DisasterRecovery
SetStorageShareSmbEnabled DISASTER_RECOVERY /
DisasterRecovery T DR
SetStorageShareNfsEnabled DISASTER_RECOVERY /
DisasterRecovery T DR
```

The recovery process attempts to restore the NAS server and the storage array settings based on the contents of the DRF. The NAS system provides the following disaster-recovery capabilities:

- Restoring the NAS server configuration (the storage arrays remain unchanged)
- Restoring storage array settings (the NAS server remains unchanged)
- Restoring both the NAS server and the storage array settings

Restoring the NAS Server Configuration

If the NAS server is replaced, the system configuration can be restored from the DRF. No user data needs to be restored to the storage array.

- 1 Verify that the new NAS server is running the same version of the NAS operating system that was previously in use.
- 2 Connect a laptop to prepare the NAS server for disaster recovery:
 - Connect a laptop with terminal emulation software to the server. Connect an RS232 null-modem to the Management Port on the server.
 - Use the terminal emulator to log in. Use the following settings:
 - Bits per second: 9600
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None
 - Press **Enter** until you see the system name and login prompt, as shown here, then log in as admin. No password is required.

```
hp nas8000
NAS OS v1.0.0
localhost login:admin
```
- 3 Follow the installation instructions in the *HP NAS 8000 Installation Guide* to configure basic network settings (IP address, Subnet, etc.) on the NAS server.
- 4 Restore the DRF file:
 - Share and set write-access permission on the DISASTER_RECOVERY volume.
 - Copy the DRF file from the backup location to the DISASTER_RECOVERY volume on the NAS server.

- 5 To activate the disaster recovery process and restore settings from the DRF, type:
`recoverSystemHeadFromDisasterRecoveryFile <name of disaster recovery file>`
- 6 To reboot the NAS server, and complete the recovery process, type:
`doSystemReboot`

Restoring Storage Array Settings

When a storage array is replaced, the recovery process attempts to format the replacement array(s) to have the same LUN and volume group configuration as the current NAS registry indicates. After the storage array is recovered, restore user data from backup tape.

Note SAN configurations cannot be automatically recovered, however, information pertinent to the recovery is saved in the DISASTER_RECOVERY volume. This information may be used to manually recovery the SAN storage configuration.

- 1 Shut down the NAS server and connect the new storage array(s):
 - If you have a direct-attach configuration, follow the installation instructions in the *HP Surestore NAS 8000 Solution Integration Manual* to connect the array(s).
 - If you have a SAN configuration, follow the instructions in the array users guide to connect the array(s).
- 2 Access the command line interface to run disaster recovery commands:
 - Connect a laptop with terminal emulation software to the server. Connect an RS232 null-modem to the Management Port on the server.
 - Use the terminal emulator to log in. Use the following settings:
Bits per second: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None
 - Press **Enter** until you see the system name and login prompt, as shown here, then log in as admin. No password is required.
hp nas8000
NAS OS v1.0.0
localhost login:admin

- 3 To activate the disaster recovery process and restore settings from the DRF, type:
`recoverSystemStorageConfig`
- 4 The recovery process checks available capacity of new storage hardware, detects which storage arrays need to be re-configured, and modifies the NAS registry to recreate LUNs, volume groups, volumes, and shares on the replacement storage array(s).
 - If the storage recovery process completes with no errors, user data may now be restored from tape onto the replacement storage array(s).
 - If the recovery process encountered errors, the configuration cannot be automatically recovered with the replacement storage array(s). At this point, you may attempt recovery again with different replacement storage array(s), or alternatively, start with a new NAS operating system and rebuild the array configurations manually.
 - If recovering on a SAN configuration, configuration information is saved in the DISASTER_RECOVERY volume in the file:
`recoverSystemStorageConfig.out`
- 5 To log out of the command line interface, type:
`exit`

Restoring the NAS Server and Storage Array

If both the server and storage array(s) fail, the following process recovers the server first, then the storage array(s).

- Recover the NAS head, as described in **Restoring the NAS Server**.
- After rebooting the NAS head, recover storage array(s) starting from step 4 in **Restoring a Storage Array**.

Note

The recovery process runs following the installation of the replacement NAS head and/or storage hardware and requires action from a system administrator.

■ The recovery process assumes that the replacement hardware is identical to the original hardware that failed. While recovery may be attempted on differing replacement hardware, or hardware of differing capacities, successful results are not guaranteed.

■ If there is a failure while recovering the storage array configuration due to the use of different storage hardware, or hardware of differing storage capacities, then the administrator will have to manually configure the replacement storage array hardware.

■ The recovery process assumes that the NAS server that is used for recovery is running the same version of the NAS operating system (at the same patch level) that was running when the DRF file was created. For example, a NAS operating system version 1.2 cannot be used to recover a configuration contained in a DRF file that was created by an earlier NAS operating system version 1.1.

The recovery process can assist with SAN-based installations by providing information required by the Administrator to manually recover volume groups and file volumes. This information is posted in the `DISASTER_RECOVERY` volume after running the text command: `recoverSystemStorageConfig`.

Integrating with Network Backup Applications



You can use third-party backup applications on any computer on the network with a tape drive attached to perform a network backup. The HP NAS 8000 supports the following backup applications:

- HP OpenView OmniBack II (page 161)
- Computer Associates ARCserve 2000 (page 165)
- Veritas Backup Exec (page 167)
- Veritas NetBackup (page 169)
- IBM Tivoli Storage Manager (page 171)
- Legato NetWorker (page 173)

Note

These backup applications have been tested to be compatible with the HP NAS 8000 device. Additionally, any backup package that can back up a CIFS or NFS mount without using the backup agent should be compatible. Contact the software vendors for compatibility information with network-attached storage devices.

Backup files are accessed using file protocols such as CIFS or NFS via the network. Backup and restore via CIFS protocols preserves both CIFS and NFS attributes. Backup and restore via NFS protocols only preserves NFS attributes.

When you run a backup, data from the NAS server transfers over the network to the backup server running the backup application, and then to the backup server-attached tape device. The backup application cannot control a tape library or other tape devices connected to the NAS server.

Note If the backup application is running under NT, the restore operation recovers both the NT and UNIX security settings for each file. If the backup application is running under UNIX, the restored NT files revert to the default user security setting, while UNIX files retain their full security settings.

The information covered in this section pertains only to specific tasks you must perform to use these applications with your HP NAS 8000 device. For general information about the backup software, refer to the user's manual that came with the backup software.

Using HP OpenView OmniBack II

Note This section discusses the OmniBack II 3.5 network backup solution only. If you are using OmniBack II 4.0 or later, we recommend that you perform backups using the OmniBack backup agent for the NAS server as described in Using the Backup Agent.

HP OpenView OmniBack II 3.5 is a network-only backup solution that provides reliable data protection and high accessibility for your data. OmniBack II offers comprehensive backup and restore functionality specifically tailored for enterprise-wide and distributed environments.

You can use OmniBack II versions 3.5 on either a Windows NT or UNIX system connected to your NAS server.

Note When you back up with a remote server, you cannot use a tape device local to the NAS server.

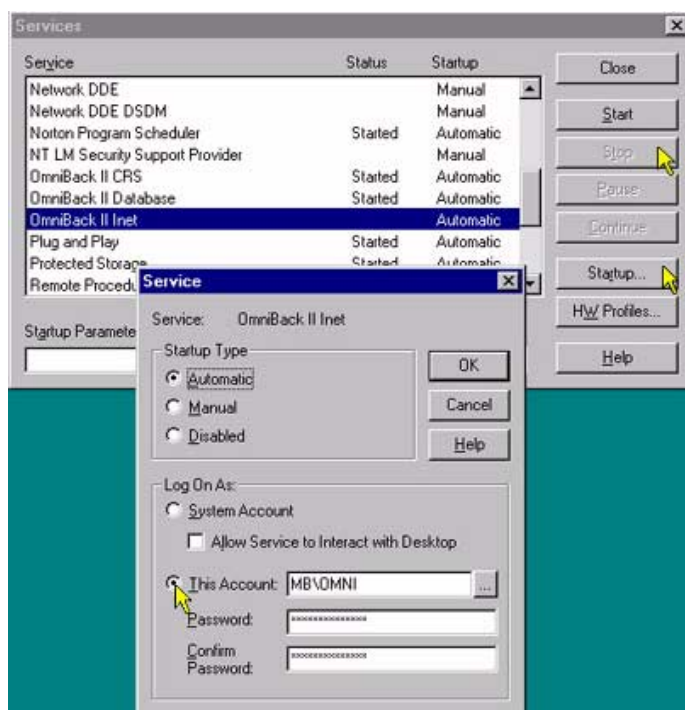
OmniBack II User Interface for Windows NT

Note For a complete discussion on backup over the network, see the *HP OpenView OmniBack II Administrator's Guide*.

Before you use OmniBack II to back up data from the NAS server, you must enable OmniBack II for Windows NT to back up remote systems.

- 1 Select **Start > Settings > Control Panel**. Double-click **Services**.
- 2 Locate the OmniBack II Inet Service, then click **Stop**.
- 3 Click **Startup**, then click **This Account**. Select a valid network administrator account. Create a password, confirm it, then click **OK**.
- 4 Click **Start** to restart the OmniBack II Inet service.

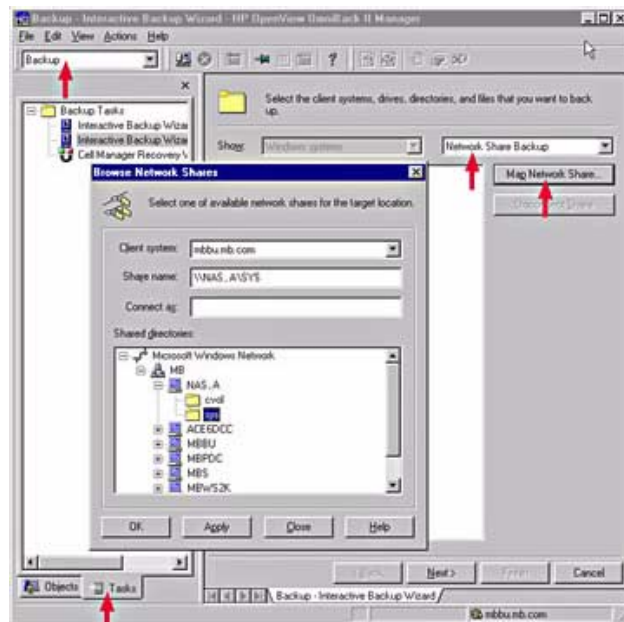
Figure 1 OmniBack II Inet Service



To back up files from the NAS server using OmniBack II for Windows NT:

- 1 Select **Start > HP OmniBack II > OmniBack II Manager**.
- 2 Verify that **Backup** is selected in the drop-down list in the top left corner of the window.
- 3 Click the **Tasks** tab on the bottom of the screen, then click **Interactive Backup Wizard**.

Figure 2 Interactive Backup Wizard



- 4 Change **File System Backup** to **Network Share Backup** in the drop-down list.
- 5 Click **Map Network Share**.
- 6 Select **Microsoft Windows Network > Domain Name > NAS Device**. In the figure above, the **Domain Name** is **MB**, and the **NAS Device** is **NAS_A**. Select the desired share.
- 7 Select the files or volumes you want to back up.
- 8 Select your backup options as you normally would, then start the backup.

OmniBack II User Interface for UNIX

Note For a complete discussion on backup over the network, see the *HP OpenView OmniBack II Administrator's Guide*.

Before you can backup with OmniBack II, you must:

- Mount on your local host machine the NAS server volumes you want to back up.
- Configure the NAS server so that the UNIX backup system is set to a trusted host on the NAS server.

To back up files from the NAS server using OmniBack II for UNIX:

- 1 Open a HP terminal window and type `xomni`, then press **Return** to start OmniBack II.
- 2 Click the **Backup** icon.
- 3 Select **Actions > Interactive Backup**.
- 4 A job editor appears. Select **Object > Add > File System** to add an object to back up. You must choose **File System** to access the NAS server.
- 5 In the **Backup File System** window:
 - a Select **Hostname** (the local backup host).
 - b Enter a **Mountpoint** (the mountpoint for the NAS volume).
 - c Enter a description.
 - d Select **Browse**, then highlight the device to back up.
 - e Click **Backup Device**, select a device, then click **OK**.
- 6 Select the files or volumes you want to back up.
- 7 Select your backup options as you normally would, then start the backup.

Using Computer Associates ARCserve 2000

ARCserve 2000 is a backup and restore management solution developed to function across various platforms (ARCserve 2000 is a product of Computer Associates International, Inc.). Check the manual that came with your software to see what platforms your edition of ARCserve 2000 supports.

You can use ARCserve 2000 on a Windows NT server connected to your NAS server.

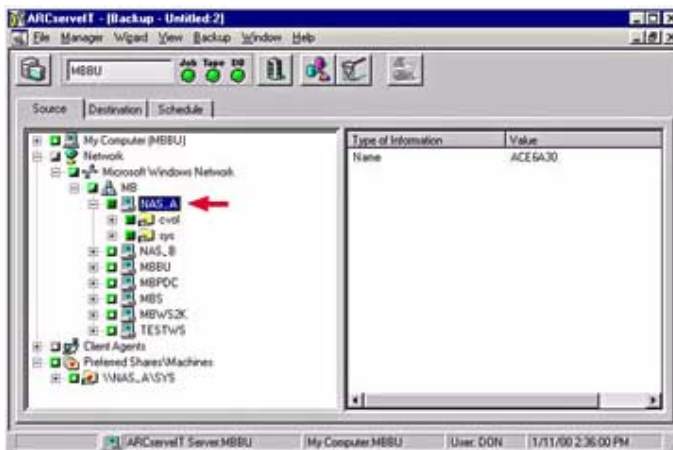
Note When you back up with a remote server, you cannot use a tape device local to the NAS server.

ARCserve 2000 for Windows NT

To back up files from the NAS server using ARCserve 2000 for Windows NT:

- 1 Open ARCserve 2000 for Windows NT.
- 2 Select **Manager > Quick Access > Backup Manager**.
- 3 Select **Network > Microsoft Windows Network > Domain Name > NAS Device**. In the figure below, the **Domain Name** is **MB**, and the **NAS Device** is **NAS_A**.

Figure 3 ARCserve Backup



- 4 Select the NAS server mount points you want to back up.
- 5 When asked for a user and password, enter any valid user and the share password as configured on the NAS server.
- 6 Select your backup options as you normally would, then start the backup.

For more information about using ARCserve 2000, see the manual that came with the software.

Using Veritas Backup Exec

Backup Exec is a high-performance data management solution for Windows NT networks (Backup Exec is a product of Veritas Software Corporation). The product provides fast, reliable backup and restore capabilities for servers and workstations across the network.

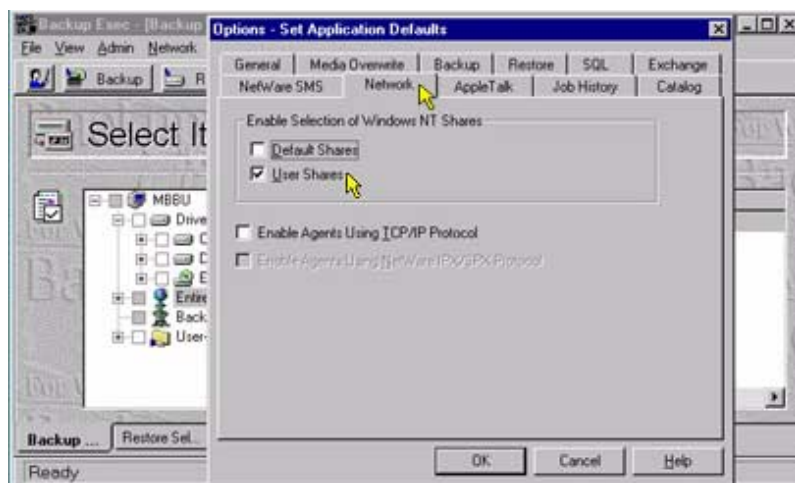
Backup Exec is available in configurations that can accommodate multiplatform networks of all sizes. Backup Exec requires a remote NT server license to allow network operations with NAS server. Check your software to see which edition you are running.

Note When you back up with a remote server, you cannot use a tape device local to the NAS server.

To back up files from the NAS server using Backup Exec Advanced Edition on a Windows NT server:

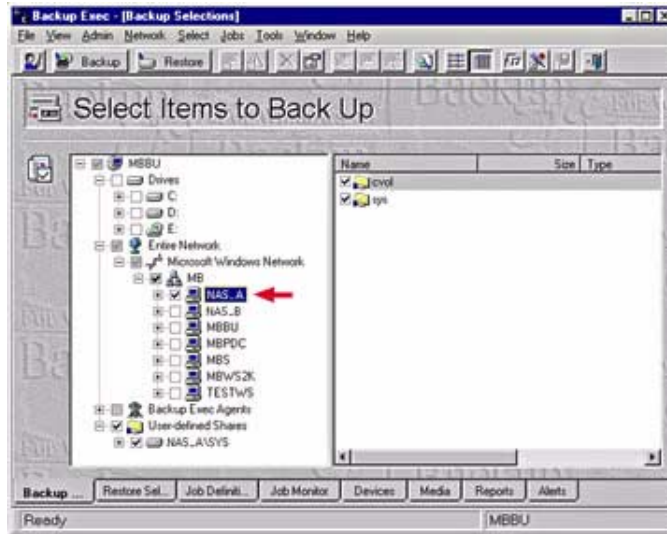
- 1 Open Backup Exec.
- 2 Select **Tools > Options**. The **Options** dialog box appears.
- 3 Click the **Network** tab, then check **User Shares**.

Figure 4 Backup Exec: User Shares



- 4 Select **Entire Network > Microsoft Windows Network > Domain Name > NAS server**. In the figure below, the **Domain Name** is **MB**, and the **NAS server Device** is **NAS_A**.

Figure 5 Backup Exec: Items to Back Up



- 5 Select the files or volumes you want to back up.
- 6 Select your backup options as you normally would, then start the backup.
- For more information about using Backup Exec, see the manual that came with the software.

Using Veritas NetBackup

NetBackup is a network based, backup and recovery tool (NetBackup is a product of Veritas Software Corporation).

You can use NetBackup on either a Windows NT or UNIX system connected to your NAS server.

Note When you back up with a remote server, you cannot use a tape device local to the NAS server.

NetBackup for Windows

- 1 Select **Start > Programs > Veritas NetBackup > NetBackup Admin**.
- 2 Select **Backup, Archive, & Restore**.
- 3 Click **Select for Backup**.
- 4 Expand the network and find the NAS server. Expand the volumes. You can only back up Windows shared volumes.
- 5 Select a volume and click **Backup > Start Backup of Marked Files**.
- 6 Select your backup options as you normally would, then start the backup.

NetBackup for UNIX

Before you can backup with NetBackup, you must:

- Mount on your local host machine the NAS server volumes you want to back up.
- Configure the NAS server so that the UNIX backup system is set to a trusted host on the NAS server.

To back up files from the NAS server using NetBackup for UNIX:

- 1 Execute `/usr/opensv/netbackup/bin/xnb`.
- 2 Verify that the Class Attributes for the backup has the **Follow NFS** option selected.
- 3 Select **Backup, Archive, & Restore**.
- 4 Click **Select for Backup**.
- 5 Expand the network and find the NAS server. Expand the volumes. You can only back up NFS mounted volumes.
- 6 Select a volume and click **Backup > Start Backup of selected files and directories**.
- 7 Select your backup options as you normally would, then start the backup.

For more information about using NetBackup, see the manual that came with the software.

Using IBM Tivoli Storage Manager

Storage Manager is a network based, backup and recovery tool (Storage Manager is a product of Tivoli Systems Inc., an IBM company).

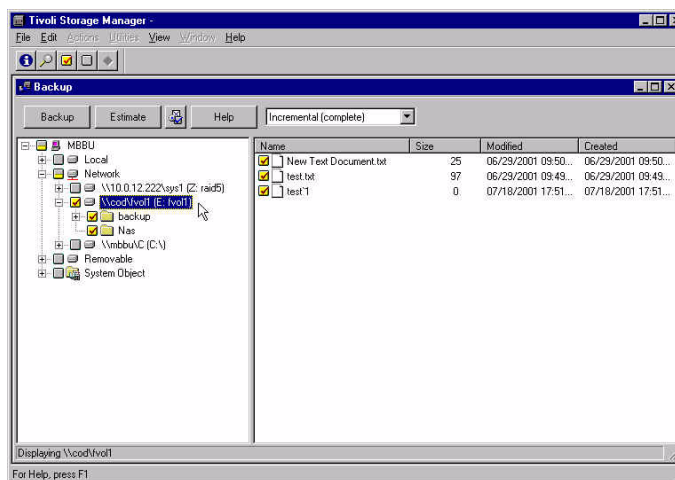
You can use Storage Manager on either a Windows NT or UNIX system connected to your NAS server.

Note When you back up with a remote server, you cannot use a tape device local to the NAS server.

Storage Manager for Windows

- 1 Select **Start > Programs > Tivoli Storage Manager > Backup Client GUI**.
- 2 Select **Backup**.
- 3 Expand the network and find the NAS server. Expand the volumes. You can only back up Windows shared volumes that have been mapped to the backup server.
- 4 Select the files, directories, or volumes you want to back up.
- 5 Select your backup options as you normally would, then start the backup.

Figure 6 Storage Manager



Storage Manager for UNIX

Before you can backup with Storage Manager, you must:

- Mount on your local host machine the NAS server volumes you want to back up.
- Configure the NAS server so that the UNIX backup system is set to a trusted host on the NAS server.

To back up files from the NAS server using Storage Manager for UNIX:

- 1 Execute `dms`.
- 2 Select **Backup Files and Directories**.
- 3 Expand the network and find the NAS server. Expand the volumes. You can only back up NFS mounted volumes.
- 4 Select the files, directories, or volumes you want to back up.
- 5 Select your backup options as you normally would, then start the backup.

For more information about using Storage Manager, see the manual that came with the software.

Using Legato NetWorker

NetWorker is a network based, backup and recovery tool (NetWorker is a product of Legato Systems, Inc).

You can use NetWorker on either a Windows NT or UNIX system connected to your NAS server.

Note When you back up with a remote server, you cannot use a tape device local to the NAS server.

NetWorker for Windows

- 1 Select **Start > Programs > NetWorker Group > Network User**.
- 2 Select **Backup**.
- 3 Expand the network and find the NAS server. Expand the volumes. You can only back up Windows shared volumes that have been mapped to the backup server.
- 4 Select the files, directories, or volumes you want to back up.
- 5 Select your backup options as you normally would, then start the backup.

Networker for UNIX

Before you can backup with Networker, you must:

- Mount on your local host machine the NAS server volumes you want to back up.
- Configure the NAS server so that the UNIX backup system is set to a trusted host on the NAS server.

To back up files from the NAS server using Networker for UNIX:

- 1 Execute `/opt/networker/bin/nwbackup`.
- 2 Select **Backup, Archive, & Restore**.
- 3 Click **Select for Backup**.
- 4 Expand the network and find the NAS server. Expand the volumes. You can only back up NFS mounted volumes.
- 5 Select a volume and click **Backup > Start Backup of selected files and directories**.
- 6 Select your backup options as you normally would, then start the backup.

For more information about using NetWorker, see the manual that came with the software.

Obtaining Product Support and Software Upgrades

10

From the Support tab, you can:

- Contact service and support for the NAS server
- View the licenses that pertain to the open source code used in the NAS server and obtain a copy of the open source code used in the NAS server operating system
- Run diagnostic tools for any attached arrays
- Upgrade software for your NAS server and any attached arrays

Contacting HP NAS Server Service and Support

HP NAS 8000's electronic services give you a fast, interactive way to access information and help about setup, configuration, installation, and operation of your product. You can:

- Access HP NAS server's support web site
- Phone customer support

For information on HP authorized resellers, visit <http://www.hp.com>, then select the **how to buy** link.

You can purchase additional NAS server hardware and upgrades through the HP Business Store at <http://www.bstore.hp.com>.

HP NAS Server Support Web Site

To access the support web site for your NAS server:

- 1 In the Command View NAS web interface, click the **Support** tab.
- 2 Navigate down the Support tree and select **Contact Information**.
- 3 Select **Actions > Online Support** to launch the HP NAS 8000 web site. (<http://www.hp.com/support/nas8000>).

From this web site, you can obtain support information and contact HP.

Contact Customer Support

To contact customer support by phone in the U.S., dial 970-635-1000. For phone numbers in other countries, see the HP NAS 8000 web site (<http://www.hp.com/support/nas8000>).

Viewing the Command View NAS License

To view the Command View NAS software license agreement:

- 1 In the Command View NAS web interface, click the **Support** tab.
- 2 Navigate down the Support tree and select **Command View NAS License**.
- 3 Select **Actions > Command View NAS License** to view the software license agreement.

Viewing Open Source Code

The NAS server makes use of Open Source (GNU, GPL, and LGPL) licensed software.

To satisfy Open Source license agreements, any modified Open Source code that the NAS server operating system uses is available through the Command View NAS web interface.

- 1 In the Command View NAS web interface, click the **Support** tab.
- 2 Navigate down the Support tree and select **Open Source**.
- 3 Select an item from the list, then select **Actions > Export Selected File** to download a copy of the source code.

Using Array Diagnostics

To launch the Command View SDM for array diagnostics:

- 1 In the Command View NAS web interface, click the **Support** tab.
- 2 Navigate down the Support tree to **Support Diagnostics** and select **<Name of Array>**.
- 3 Select **Actions > Array Diagnostics** to launch the Command View SDM web interface.

Upgrades

You should periodically ensure that you have the latest operating system, user interface, and documentation on your system. From the Support tab, you can obtain these upgrades for your NAS server and storage array.

Upgrading NAS Server Software

To obtain an upgrade to the NAS server's software (operating system and applications), contact your Hewlett-Packard representative or go to the support web site (<http://www.hp.com/support/nas8000>).

If you have obtained a software upgrade CD from HP and wish to install it, follow these steps:

- 1 In the Command View NAS web interface, click the **Support** tab.
- 2 Navigate down the tree to the **Upgrades** section and select **NAS Operating System**.
- 3 Select **Actions > Upgrade NAS Server**.
- 4 Navigate to where the image is stored on the CD, and click the file.
- 5 Click **Open** to upgrade the NAS server software with this image.
- 6 You are asked to confirm this operation. If you click **Yes**, the new image is copied to the NAS server, your browser window closes, and the NAS server reboots to the new operating system. When the reboot completes, open a new browser and enter the IP address of the HP NAS 8000 in the address or location field.

To obtain a software upgrade from the support web site:

- 1 In the Command View NAS web interface, click the **Support** tab.
- 2 Navigate down the tree to the **Upgrades** section and select **NAS Operating System**.
- 3 Select **Actions > Retrieve Latest Image from Web** and download the image.
- 4 Follow steps 3-6 above to complete the upgrade.

Upgrading Storage Array Firmware

To upgrade your storage array firmware, you need to launch the Command View SDM web interface.

- 1 In the Command View NAS web interface, click the **Support** tab.
- 2 Navigate down the tree to **Upgrades**, then select **<Name of Array>**.
- 3 Select **Actions > Upgrade Array** to launch the Command View SDM web interface.

For details about how to complete the upgrade, see your storage array documentation.

NAS 8000 System and Hardware Upgrades



System Upgrades

Upgrading to a High-Availability System

HP NAS 8000 direct-attach or single-server SAN configurations can be upgraded after the time of purchase to include high-availability features.

Upgrading to a high-availability system requires the following procedures:

- 1 Purchase and install an high-availability hardware upgrade kit
- 2 Receive a high-availability authorization RPM from HP and install the upgrade software
- 3 Restart NAS servers to activate high-availability features
- 4 Configure your storage system with Failover Packages

For more information or to order an high-availability upgrade kit, contact your HP sales representative.

Hardware Upgrades and Replacements

This section includes procedures for upgrading and replacing field replaceable units (FRUs) that require additional configuration of the HP NAS 8000 solution. It describes the procedures for:

- NAS server upgrades
- Storage array upgrades
- Tape library upgrade
- UPS upgrade

For information on HP authorized resellers, visit <http://www.hp.com> and select the **how to buy** link.

You can purchase additional HP NAS 8000 hardware and upgrades through the HP Business Store at <http://www.bstore.hp.com>.

NAS Server Upgrades

The following upgrades may be made to the HP Netserver LT6000r. These upgrades require additional configuration of the HP NAS 8000 solution after the hardware installation is complete:

Adding NICs

The LT6000r has one integrated network port. The HP NAS 8000 solution can also ship with additional NICs ordered at the time of purchase.

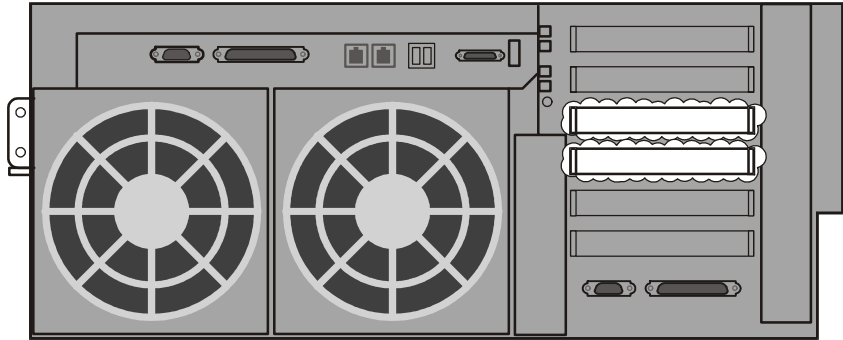
NIC upgrade kits are also available after purchase. Contact your HP sales or support representative for a list of supported NICs.

To install additional NICs in the NAS server:

- 1 Power down the system in the following sequence before installing the new card:
 - NAS server(s)
 - Quorum server (for high-availability configurations)
 - Array
 - FC switch (for high-availability configurations)
 - Library
 - UPS

- 2 Follow the instructions that come with your NIC upgrade kit to install the new card(s) into the reserved PCI slots 3 and 4 that have been allocated for NIC expansion.

Figure 1 NAS Server Rear View



Note You may install any supported NIC into slots 3 or 4 in any order; however, the HP NAS 8000 operating system will assign ports in the order the drivers are loaded, not in the order the hardware is initialized.

- 3 Power up the system in this sequence:
 - UPS
 - Library
 - FC switch (for high-availability configurations)
 - Array
 - Quorum server (for high-availability configurations)
 - NAS server(s)

Assigning IP Addresses

After you have installed NICs, you must assign IP addresses.

- 1 In the Command View NAS web interface, click the **Configuration** tab.
- 2 Navigate down the tree to **Networking Settings > TCP/IP** and select **IP Addresses**. Your current NIC configuration is displayed.
- 3 Enter the IP address for the new NICs in the address location field.

For more information, see “Defining IP Addresses” on page 54.

Firmware Upgrades

Upgrading the firmware of the NAS server requires attaching a keyboard and monitor. See the HP Netserver LT6000r support site to acquire the necessary disk images and upgrade instructions:

- Firmware upgrades <http://www.hp.com/support/nas8000>

Standard Server Upgrades

Additional standard upgrades may be made to the NAS server. These upgrades do not require any additional configuration of the HP NAS 8000 solution. Please contact your HP support representative for information regarding supported server configurations.

For additional upgrade information, see:

- Accessories and upgrades <http://www.hp.com/support/nas8000>
- Replaceable parts <http://www.hp.com/support/nas8000>

Storage Array Upgrades

Adding Disks

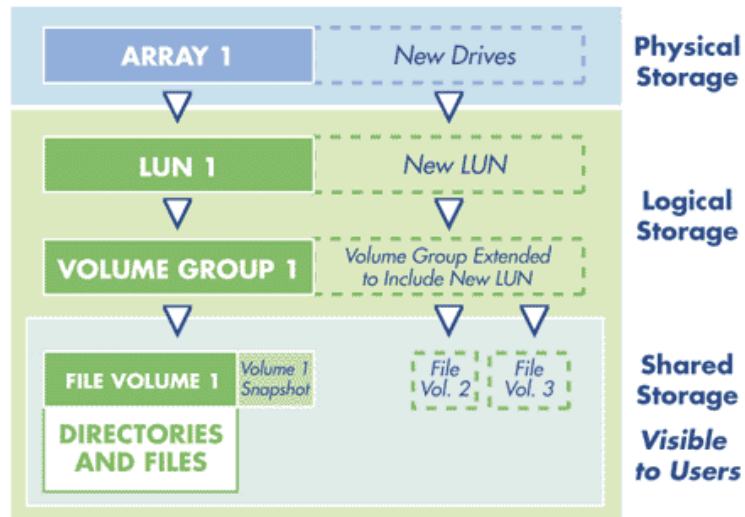
To increase capacity, additional disks may be added to the storage array in the HP NAS 8000 solution. If you have VA7400 series arrays, up to six DS2400 disk enclosures may also be added to each array. Instructions for these procedures appear in the *HP Surestore VA7100 and VA7400 User and Service Guide* (see http://www.hp.com/cposupport/manual_set/lpg28817.pdf). Please contact your HP support representative for information on supported configurations.

Modifying Storage Settings

The storage space on the new disks must be made accessible to the server and users. This can be done in two ways:

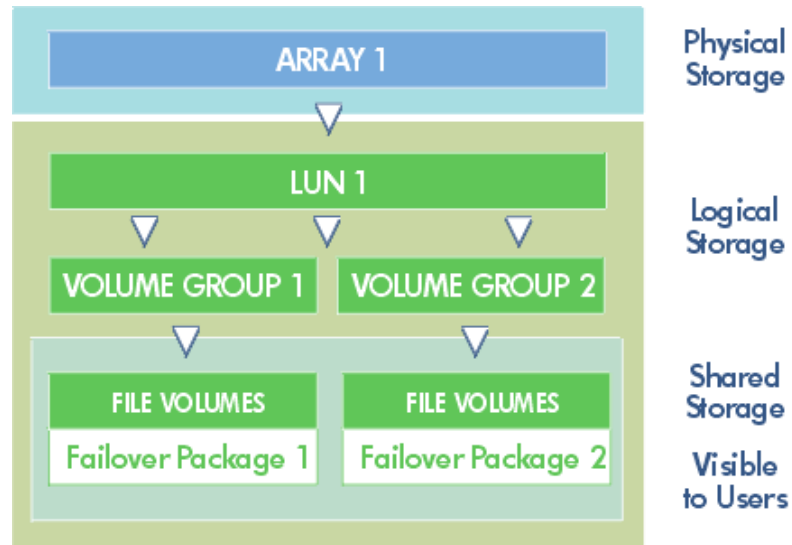
- Expanding an existing volume group to include the new LUN.

Figure 2 Expanding a Volume Group



- Creating a new volume group.

Figure 3 Creating a Volume Group



To make the additional storage accessible to the server and users:

- 1 Create a new LUN (logical drives) that includes all of the space available on the new disk(s):
 - a From the **Storage** tab, navigate down the tree to **Storage Array Summary**, then select a storage array.
 - b Select **Actions > Create New LUN**.
 - c Allocate all of the new space to this LUN.
- 2 Expand a volume group to include the new space or create a new volume group:
 - a From the **Storage** tab, navigate down the tree and select **Volume Groups**.
 - b Select the volume group to which you will add the new space by clicking the row.

- c Select **Actions > Edit Selected Volume Group.**
 - or
 - Select **Actions > Create New Volume Group.**
 - d Add the new LUN to the volume group.
 - 3 Create file volumes:
 - a From the **Storage** tab, navigate down the tree to the **File Volumes**, then select **File Volumes Summary**.
 - b Select **Actions > Create New File Volume.**
 - c Assign space to volume.
 - d Assign a volume name and SNMP trap threshold.
 - 4 Assign sharing access to volumes or directories:
 - a From the **Storage** tab, navigate down the tree and select **Shares/Export**.
 - b Select **Actions > Create New Share/Export.**
 - c Select a share protocol (Windows, NFS) and assign hosts and settings.

Tape Library Upgrade

Adding a Tape Library

Tape libraries can be added to the HP NAS 8000 after the initial purchase and installation.

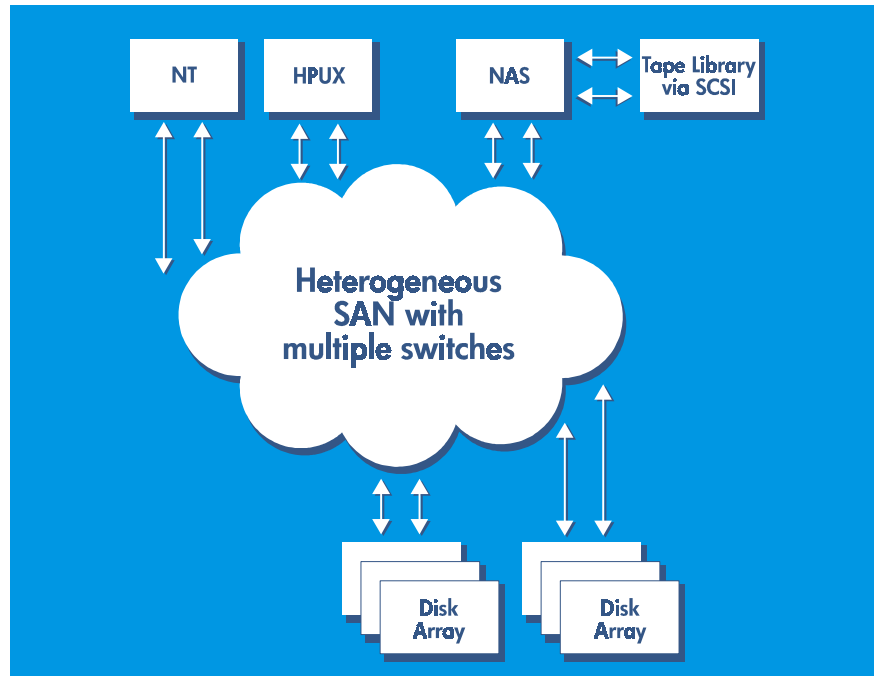
Installing SCSI or FC HBA Cards

Adding a tape library to a system that was not purchased with one requires installing SCSI or FC HBA cards in the NAS server. Contact your HP sales or support representative for a list of supported HBAs.

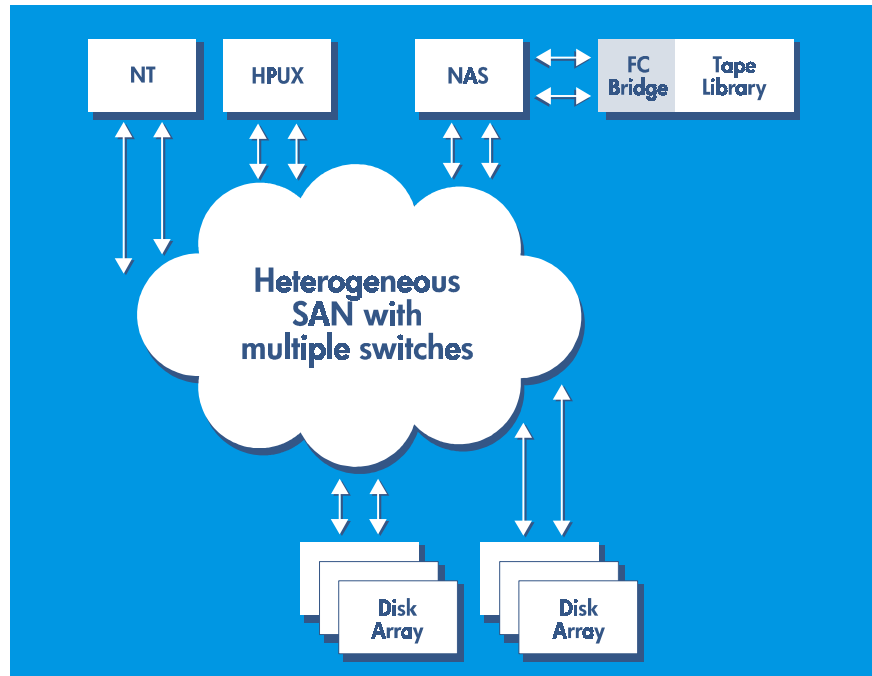
To add a new tape library:

- 1 Power down the system in the following sequence before installing the new cards:
 - Server
 - Array
 - UPS
- 2 Follow the instructions that come with your HBA cards to install the new cards into the reserved PCI slots 1 and 2.
- 3 Follow the instructions that come with the tape library to connect the library to the NAS server or SAN in one of the following configurations:

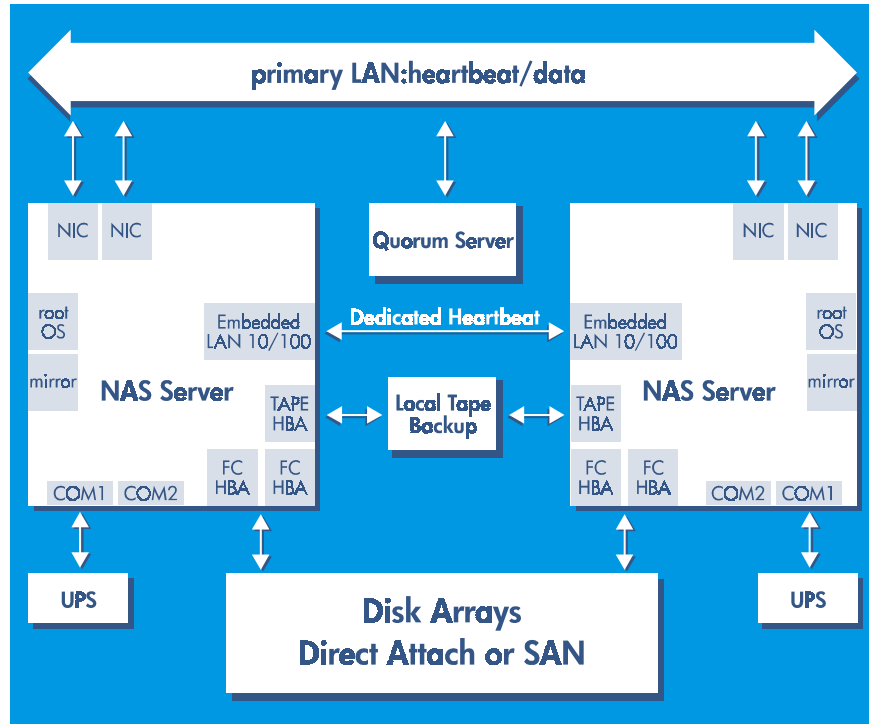
- NAS server connected to tape libraries via SCSI cards:



- NAS server connected to tape libraries via the point-to-point FC:



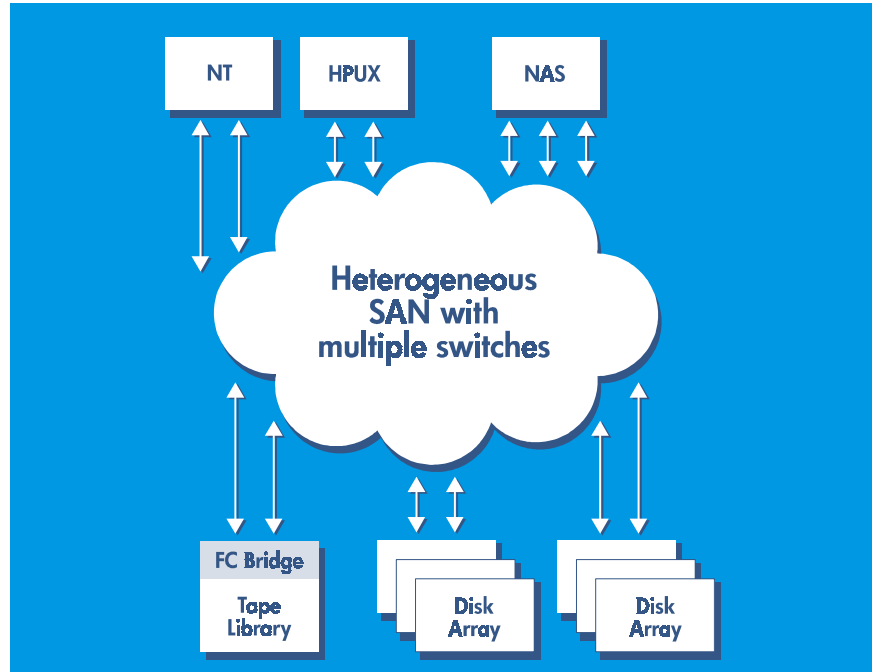
- High-availability NAS servers connected to shared tape library via SCSI or FC:



- NAS server connected to tape libraries via the FC fabric.

Note

Note: HP NAS 8000 servers can not share the same tape library with other components on the SAN.



4 Power up the system in this sequence:

- UPS
- Library
- Array
- Server

Using the Command View NAS web interface, you can install and enable HP Omniback II v4.1 backup agent software for local backup.

Firmware Upgrades

For instructions for upgrading firmware, see your tape library documentation.

UPS Upgrade

Adding a UPS

The following UPS systems can be added to the HP NAS 8000 solution after the time of purchase. The specific model of UPS recommended is customized each region:

- American Power Conversion (APC) Symmetra RM (8U)
- American Power Conversion (APC) Symmetra RM (15U)
- American Power Conversion (APC) Symmetra

To install the UPS on the HP NAS 8000 solution, follow these steps:

- 1 Follow the instructions that came with the UPS for power requirements.
- 2 Power down all of the solution components in the following sequence before installing the UPS:
 - NAS server(s)
 - Quorum server (for high-availability configurations)
 - Array
 - FC switch (for high-availability configurations)
 - Library
- 3 Install the UPS in the bottom of the rack to avoid having a top-heavy rack and to eliminate the risk of tip over.
- 4 Connect the communications port on the UPS to the server's COM1 serial port.
- 5 Plug components into PDU on UPS.
- 6 Connect power to UPS.
- If you are installing the Symmetra RM UPS:
 - If the planned power load is less than or equal to 5 kVA, plug the line into an appropriate outlet.
 - If the planned power load is greater than 5 kVA, a qualified electrician must hard wire the input power.
- If you are installing the Symmetra UPS:
 - Regardless of the power load, a qualified electrician must hard wire the input power.

7 After the UPS is installed, power up the system components in this sequence:

- UPS
- Library
- Switch(es)
- Array(s)
- Server(s)

Access the Command View NAS web interface to configure UPS communications.

UPS Product Information

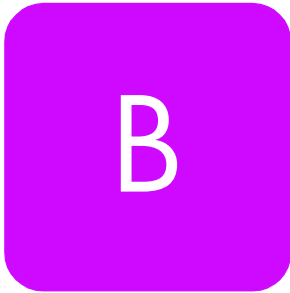
For additional information on APC UPS products contact:

American Power Conversion
132 Fairgrounds Road
West, Kingston, RI 08892
<http://www.apcc.com>

Technical Support and Product Information:
1-800-800-4272

APC HP Sales Representative:
508-883-1916
508-883-6662 FAX

SNMP Trap Definitions



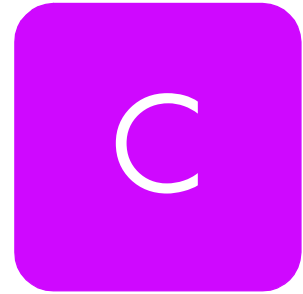
If you have a NAS server integrated with network management software, the following traps are sent to the management station in the event of a hardware failure or system alert. See “Defining SNMP Alerts” on page 70 for information on defining the server.

Trap	Definition
hpHttpUnknownHealthTrap	Sent when the device’s health is unknown. The device health object in the hpHttpMgDeviceTable should be set to unknown, then the trap should be sent. The trap includes the device’s index in the table, the SysObjID, the GlobalUniqueID, and, if available, the ManagementURL, the ManagementURLLabel, the deviceSpecificEventCode and the deviceSpecificEventFRU. This allows the trap receiver to gain additional information about the device by accessing the device management software or the management software to launch the device management software.
hpHttpOKHealthTrap	Indicates that the device's health has changed to OK. The device health object in the hpHttpMgDeviceTable should be set to OK, then the trap should be sent. The trap includes the device's index in the table, the SysObjID, the GlobalUniqueID, and, if available, the ManagementURL, the ManagementURLLabel, the deviceSpecificEventCode and the deviceSpecificEventFRU. This allows the trap receiver to gain additional information about the device by accessing the device management software or it allows the management software to launch the device management software.

Trap	Definition
hpHttpWarningHealthTrap	<p>Indicates that the device's health has changed to warning. The criteria for a warning state are device specific. The device health object in the hpHttpMgDeviceTable should be set to warning, then the trap should be sent. The trap includes the device's index in the table, the SysObjID, the GlobalUniqueID, and, if available, the ManagementURL, the ManagementURLLabel, the deviceSpecificEventCode and the deviceSpecificEventFRU. This allows the trap receiver to gain additional information about the device by accessing the device management software or it allows the management software to launch the device management software.</p>
hpHttpCriticalHealthTrap	<p>Indicates that the device's health has changed to critical. The criteria for critical health are device specific. The device health object in the hpHttpMgDeviceTable should be set to critical, then the trap should be sent. The trap includes the device's index in the table, the SysObjID, the GlobalUniqueID and, if available, the ManagementURL, the ManagementURLLabel, the deviceSpecificEventCode and the deviceSpecificEventFRU. This allows the trap receiver to gain additional information about the device by accessing the device management software or it allows the management software to launch the device management software.</p>
hpHttpNonRecoverableHealthTrap	<p>Indicates that the device's health has changed to non-recoverable and the device needs to be rebooted. All management software should report this as a critical error. The device health object in the hpHttpMgDeviceTable should be set to unknown, then the trap should be sent. The trap includes the device's index in the table, the SysObjID, the GlobalUniqueID, and, if available, ManagementURL, the ManagementURLLabel, the deviceSpecificEventCode and the deviceSpecificEventFRU. This allows the trap receiver to gain additional information about the device by accessing the device management software or it allows the management software to launch the device management software.</p>

Trap	Definition
hpHttpDeviceAddedTrap	Sent whenever a device is added to the MIB. The key element in this trap is the hpHttpMgDeviceIndex that allow the management software to find the device easily and add it to the managed environment. If there is no device management software supported via a URL, both hpHttpMgDeviceManagementURL and hpHttpMgDeviceManagementURLLabel should be null.
hpHttpDeviceRemovedTrap	Sent whenever a device is removed from the MIB. Key elements in this trap are hpHttpMgDeviceIndex and hpHttpMgDeviceSysObjID that allow the management software to find the device easily and remove it from the managed environment.

Legal Information



Acknowledgments

The following acknowledgments pertain to software used in the HP Surestore Command View NAS 8000 software:

Java

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Libedit

Copyright (c) 1992, 1993
The Regents of the University of California
All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

TCLReadline

Copyright (c) 1998 - 2000, Johannes Zellner

johannes@zellner.org

All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

HP Surestore Software License Agreement

IMPORTANT - READ CAREFULLY BEFORE USING THIS PRODUCT. THIS AGREEMENT APPLIES ONLY TO HEWLETT-PACKARD PROPRIETARY SOFTWARE AND THIRD PARTY SOFTWARE NOT SPECIFICALLY IDENTIFIED AS BEING LICENSED UNDER A SEPARATE AGREEMENT. SOME LICENSE AGREEMENTS FOR THIRD PARTY SOFTWARE ARE PROVIDED IN THE SOFTWARE ITSELF.

PROCEEDING AND USING THIS PRODUCT IS AN INDICATION THAT YOU ACCEPT THESE TERMS AND CONDITIONS AND IS A REPRESENTATION BY YOU THAT YOU HAVE THE AUTHORITY TO ACCEPT THEM. IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU SHOULD PROMPTLY RETURN THE UNUSED PRODUCT AND YOUR MONEY WILL BE REFUNDED.

This End-User License Agreement ("Agreement") is a binding legal agreement between you (either an individual or a legal entity) and Hewlett-Packard. By using this Hewlett-Packard software (the "Software") product, you agree to be bound by the terms of this Agreement. (The term Software includes the computer software, the associated media, any printed materials, and any "on-line" or electronic documentation.) If you do not agree to the terms of this Agreement, Hewlett-Packard is unwilling to license the Software to you. In such event, you may not install, use or copy the Software, and you should promptly return the unused product(s) for a refund.

The Software is protected by copyright laws and international copyright treaties as well as other intellectual property laws and treaties. The Software is licensed to you, not sold. Hewlett-Packard retains all right and title to the Software and related documentation.

1 GRANT OF LICENSE: This Agreement grants you the following rights:

- **Software:** You may install and use one copy of the Software on one server computer.
- **Back-Up Copy:** You may make one (1) back-up copy of the Software. You may use the back-up copy solely for archival purposes. You must clearly label any such copy with Hewlett-Packard's copyright notice and any other proprietary legends that appear on the original copy. The archival copy must be kept in your possession and is the property of Hewlett-Packard.

2 DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

- **Limitations on Copying and Distribution:** Except as provided in section 1 above, you may not copy, transmit, or distribute the Software, except and only to the extent that such activity is expressly permitted by applicable law despite this limitation.
- **Limitations on Reverse Engineering and Modification:** You may not reverse compile, reverse engineer, decompile, disassemble, convert to a humanly comprehensible form, modify or create works derivative of the Software. You may not disguise, obfuscate the Software in order to use it elsewhere. If the Software is serialized, you may not modify or disable the serial number features or copy protection mechanisms contained in the Software.
- **Separation of Components:** This Software is licensed as a single product. Its components may not be separated for use on more than one computer.
- **Sublicense, Rental and Third Party Use:** You may not sublicense, rent, timeshare, loan or lease the Software, or directly or indirectly permit a third party to use or copy the Software.
- **Software Transfer:** You may not sell, sublicense or otherwise transfer the Software. Your license will automatically terminate upon any attempt to transfer the Software. If you transfer, sell or otherwise dispose of the product upon which this Software is fixed, you must erase the Software before any such transfer or disposal. You will make reasonable efforts to protect the confidentiality of the Software.
- **Export:** You may not export the Software without prior written approval from Hewlett-Packard. If the Software was purchased in the United States of America, you agree to comply with all applicable United States laws and regulations pertaining to export controls. If the Software was purchased outside the U.S., you may not re-export the Software except as permitted by the laws of the United States and the laws of the jurisdiction in which you purchased the software.
- **Termination:** Without prejudice to any other rights, Hewlett-Packard may terminate this Agreement if you fail to comply with the terms and conditions set forth in this Agreement. In such event, you must return all copies of the Software and all of its components and documentation to Hewlett-Packard or certify that you have destroyed all such copies.

- 3 **COPYRIGHT:** All title and copyrights in and to the Software (including, but not limited to, any images, photographs, animations, video, audio, music,

text, incorporated in the Software, the accompanying printed materials, and any copies of the Software) are owned by Hewlett-Packard or its suppliers or licensors. You may not copy the printed materials accompanying the Software.

- 4 **U.S. GOVERNMENT RESTRICTED RIGHTS:** The Software and documentation have been developed entirely at private expense and are provided as "Commercial Computer Software" or "restricted computer software". Use, duplication or disclosure by the U.S. Government or a U.S. Government subcontractor is subject to the restrictions set forth in subparagraph (c) (I) (ii) of the Rights in Technical Data and Computer Software clauses in DFARS 252.227-7013 or as set forth in subparagraph (c) (1) and (2) of the Commercial Computer Software -Restricted Rights clauses at FAR 52.227-19, as applicable. The Contractor is Hewlett-Packard Company, 3000 Hanover Street, Palo Alto, California 94304.
- 5 **LIMITED WARRANTY:** Hewlett-Packard warrants that the Software will perform substantially in accordance with the applicable Hewlett-Packard published documentation prevailing at the time of shipment for a period of ninety (90) days from the date of receipt. Hewlett-Packard warrants that any media accompanying the Software will be free from defects in materials and workmanship under normal use and service for a period of ninety (90) days from the date of receipt. Any implied warranties on the Software and media are limited to ninety (90) days. Some states or jurisdictions do not allow limitations on the duration of an implied warranty, so the above limitation may not apply to you.
- 6 **CUSTOMER REMEDIES:** Hewlett-Packard's entire liability and your exclusive remedy shall be, at Hewlett-Packard's option, either (a) return of the price paid, or (b) repair or replacement of the Software that does not meet the limited warranty in section 5 above and which is returned to Hewlett-Packard with a copy of your receipt. Any replacement Software will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.
- 7 **NO OTHER WARRANTIES:** YOU ACKNOWLEDGE AND AGREE THAT THE USE OF THE SOFTWARE IS AT YOUR OWN RISK. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HEWLETT-PACKARD AND ITS SUPPLIERS AND LICENSORS DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. HEWLETT-PACKARD DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS,

OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE AND RELATED DOCUMENTATION WILL BE CORRECTED, FURTHERMORE, HEWLETT-PACKARD DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE RESULTS OF THE USE OF THE SOFTWARE OR RELATED DOCUMENTATION IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY HEWLETT-PACKARD OR A HEWLETT-PACKARD AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. EXCEPT AS OTHERWISE PROVIDED IN THIS AGREEMENT, SHOULD THE HEWLETT-PACKARD SOFTWARE PROVE DEFECTIVE, YOU (AND NOT HEWLETT-PACKARD OR A HEWLETT-PACKARD AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHERS WHICH VARY FROM STATE OR JURISDICTION TO STATE OR JURISDICTION.

- 8 NO LIABILITY FOR CONSEQUENTIAL DAMAGES:** TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL HEWLETT-PACKARD OR ITS SUPPLIERS OR LICENSORS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR INDIRECT DAMAGES FOR PERSONAL INJURY, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF HEWLETT-PACKARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, HEWLETT-PACKARD'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS AGREEMENT SHALL BE LIMITED TO THE PRICE PAID FOR THE SOFTWARE. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.
- 9 INDEMNITY:** You agree to indemnify and hold Hewlett-Packard and its suppliers and licensors harmless from and against any and all claims of any kind (along with attorney's fees and litigation costs), including but not limited to, personal injury or property damage arising out of, resulting from, or in connection with results you have obtained through your negligent use or misuse of the Software.

- 10 GOVERNING LAW:** This Agreement is governed by and construed in accordance with the laws of the State of California, U.S.A as applied to agreements entered into and wholly performed within California between California residents. This Agreement shall not be governed by the 1980 U.N. Convention on Contracts for the International Sale of Goods.
- 11 COMPLETE AGREEMENT:** This Agreement is the entire agreement between Hewlett-Packard and you with respect to the Software. THE ACCEPTANCE OF ANY PURCHASE ORDER PLACED BY YOU IS MADE CONDITIONAL ON YOUR AGREEMENT TO THE TERMS SET FORTH IN THIS AGREEMENT, AND HEWLETT-PACKARD AGREES TO FURNISH THE SOFTWARE ONLY UPON THESE TERMS AND NOT UPON THOSE IN YOUR PURCHASE ORDER. This Agreement replaces all prior understandings and agreements, whether written or oral. This agreement may not be modified unless Hewlett-Packard and you both assent in writing.
- 12 SEVERABILITY:** If for any reason a court of competent jurisdiction finds any provision or part of any provision of this Agreement unenforceable, that part or provision shall be enforced to the maximum extent permitted by law so as to effect the intent of the parties, and the remainder of the agreement shall continue in full force and effect.

Safety and Regulatory Information

The HP NAS 8000 solution consists of a number of component items (servers, disk arrays, and so on). Each of these component items have been independently tested for regulatory approval.

Refer to the Regulatory Information statements and Certificates of Conformity contained within the individual component manuals shipped with your system.

Note

Customers are not expected to troubleshoot individual components. For troubleshooting purposes, individual component manuals are included for reference purposes only.

HP NAS Server Warranty Information

Warranty Information

Standard Limited Warranty

The HP Surestore NAS 8000 standard warranty includes the following:

- Two-year limited warranty
- Same day on-site service for certain repairs (not available in certain geographic areas*; see table below)

See the Hewlett-Packard Hardware Limited Warranty on the following page for a complete description of the standard warranty.

*In HP-Excluded Travel Areas (where geographical obstacles, undeveloped roads, or unsuitable public transportation prohibit routine travel) service is provided on a negotiated basis at extra charge. However, HP Support Options and other enhanced services may follow different guidelines. Contact HP or your authorized HP reseller for more information.

Zone	Distance from HP Office	Response Time
1-3	100 miles (160 km)	Same business day
4-5	200 miles (320 km)	Next business day
6	300 miles (480 km)	Second business day
	> 300 miles (> 480 km)	To be negotiated

Warranty Upgrades

HP offers warranty upgrades to provide a higher level of response or repair time commitment for your HP Surestore NAS 8000. For more information on upgrading your warranty, contact your local HP sales representative or authorized reseller.

Warranty Contacts U.S. and Canada

For hardware service and telephone support, contact:

- An HP-authorized reseller
or
- In the U.S., HP Customer Support Center at 970-635-1000, 5 AM to 5 PM, M-F.
Outside the U.S., see <http://www.hp.com/support/nas8000>

Current Support Information

For the latest support information, see:
<http://www.hp.com/support/nas8000>

Preparing for a Support Call

If you must call for assistance, gathering the following information before placing the call will expedite the support process:

- Product model name and number
- Product serial number
- Applicable error messages from system or diagnostics
- Client operating system type and revision

Hewlett-Packard Limited Warranty Statement

HP warrants to you, the end-user Customer, that HP Surestore NAS 8000 hardware components and supplies will be free from defects in material and workmanship under normal use after the date of purchase for two years. If HP or Authorized Reseller receives notice of such defects during the warranty period, HP or Authorized Reseller will, at its option, either repair or replace products that prove to be defective. Replacement parts may be new or equivalent in performance to new.

Should HP or Authorized Reseller be unable to repair or replace the hardware or accessory within a reasonable amount of time, Customer's alternate remedy will be a refund of the purchase price upon return of the HP Surestore NAS 8000.

Replacement Parts Warranty

HP replacement parts assume the remaining warranty of the parts they replace. Warranty life of a part is not extended by means of replacement.

Items Not Covered

Your HP Surestore NAS 8000 warranty does not cover the following:

- Products purchased from anyone other than HP or an authorized HP reseller
- Non-HP products installed by unauthorized entities
- Consumables, such as batteries
- Customer-installed third-party software
- Routine cleaning, or normal cosmetic and mechanical wear
- Damage caused by misuse, abuse, or neglect
- Damage caused by parts that were not manufactured or sold by HP
- Damage caused when warranted parts were repaired or replaced by an organization other than HP or by a service provider not authorized by HP

Command View SDM Limitations



The Command View Storage Device Manager (SDM) software is integrated with the Command View NAS web interface and resides on the NAS server. It manages the storage on any of the attached arrays. You can access the Command View SDM from the Storage, Status, and Support tabs. The Command View SDM lets you:

- Edit or manage advanced storage features on the array
- Monitor the status of the arrays
- Download new firmware

You should only access the HP Command View SDM web interface when it is called up by the Command View NAS interface. Features available in this software can damage or delete data from your arrays. Always pay attention to warnings that are displayed by the software.

Command View SDM is launched by the Command View NAS interface for the following reasons:

- **Status (Failed State)** — If there is failure in the storage array hardware, the Command View NAS interface will not provide any details. Command View SDM provides details about where within the array the fault has occurred. This access is for information only.
- **Diagnostics (Support Tasks)** — Diagnostic tools in Command View SDM are available to assist with isolating problems. To perform diagnostics on the storage array, the Command View NAS interface will start the Command View SDM interface with the “diagnostic” tab selected. This task should only be performed by an HP service representative.
- **Firmware Upgrade (Support Tasks)** — The Command View SDM interface “download” tab is accessed to upgrade storage array firmware. This task should only be performed by an HP service representative.
- **Initial System Configuration** — During initial system configuration, the storage array settings should be verified using the Virtual Front Panel

(VFP) using a laptop connection, not the Command View SDM interface. This task should only be performed by an HP service representative.

The following capabilities of the Command View SDM interface are potentially dangerous to the data in the NAS 8000 configuration and should never be used.

LUN Management — All LUN management tasks should be performed using the Command View NAS interface. The following features of the Command View SDM interface can destroy data on the system:

- **Delete LUN** — This feature has the most potential for catastrophic results. If LUNs are deleted using Command View SDM, all data within the LUN will be lost.
- **Create Business Copy (Snapshot)** — Business copies (hardware snapshots) are not supported by the NAS 8000 solution. If a business copy snapshot is created, the storage capacity allocated to the snapshot will not be available for use.
- **LUN Permissions** — If device-based LUN security is enabled, it will not be possible to access the storage arrays from the NAS server.

Configuration — These features are set during initial system setup. Once set, they should *not* be changed.

- **Host Port Behavior** — This is set to the correct value during initial configuration and should not be changed. If this is changed, the storage arrays will not communicate with the NAS server. This task should be performed by an HP service representative.
- **Host Port ID** — This is the Fibre Channel bus address. It is set to be a valid address that does not conflict with other devices on the bus during initial installation. Changing this value has unpredictable results.
- **Data Resiliency** — Changing this value could result in performance changes and jeopardizes the integrity of the data stored on the device in the event of a component or power failure.
- **Automatic include/format/spare** — These settings control what happens how new disk drives are handled when they are inserted into the storage array. Changing these settings may result in new storage not being visible to the NAS server.
- **Auto Rebuild** — This setting controls what happens when a drive fails (if an auto rebuild of the RAID set occurs). Changing the value will require manual intervention to rebuild the RAID after a drive failure.

Diagnostics — These features provide diagnostic tools. Diagnostics should be performed by an HP service representative.

- **Array Shutdown** — This setting prevents the storage array from accepting any I/O. This will eventually cause all file system requests from the server to fail. Data should not be lost, but applications using the storage will no longer have access to the device.
- **Array Reset/Restart** — This feature provides hard and soft resets of the storage array. If a reset takes too long file system requests from the server may fail. Data should not be lost, but applications using the storage will lose access to the device until it is again ready.
- **Down A Disk** — This feature logically “removes” a disk from the array (causing it to not be used). This may cause an array RAID set rebuild. “Downing” multiple disks could cause data to become unavailable.

The following table lists all of the features on the Command View SDM web interface and indicates what, if any, limitations exist in conjunction with the HP NAS 8000 solution.

Table 1 Command View SDM Limitations

Tab	Page	Feature	Limitations
Identity			No Limitations
Status	Array Status	All	No Limitations
	Component Status	All	No Limitations
	Capacity	All	No Limitations

Table 1 Command View SDM Limitations

Tab	Page	Feature	Limitations
LUN Management	Logical LUNs	Create	Use the Command View NAS interface to create LUNs in direct-attach configurations. Use the storage array software to create LUNs in SAN configurations.
		Permissions	Do not use this feature. It is not supported in the HP NAS 8000 configuration.
		Delete	Danger: LUNs should only be deleted using the Command View NAS interface to ensure they are not being used by any Volume Group. If a LUN is deleted from Command View SDM, it is possible to delete storage and permanently destroy data.
		Create Copy	Warning: See Business Copy below.
	Business Copy	All	Warning: Do not use Business Copy. Data in Business Copy snapshots is not recognized by the NAS 8000. The Command View NAS interface provides a snapshot feature which should be used for making snapshots of data. The Command View NAS snapshot features is as fast as Business Copy and provides superior space utilization.
	Secure Manager	All	Do not use Secure Manager in direct attach configurations. Secure Manager is used to assign LUNs to the NAS 8000 in a SAN configurations.

Table 1 Command View SDM Limitations

Tab	Page	Feature	Limitations
Configuration	General Settings	Alias Name	No Limitations
		Data Resiliency	Warning: This is set to <i>Normal</i> . Do not changes this setting. Changing this can affect the integrity of the data in the event of a system crash or power failure.
		Automatic Include	Do not turn this feature off. New disc drives may not be recognized.
		Auto Format Drive	Do not turn this feature off. New disc drives may not be available.
		Subsystem Level RAID Control	This is set to AutoRAID. You may choose any setting. Be sure to understand the storage capacity & performance implications before changing this setting.
		Hot Spare Mode	This is set to Automatic. Do not change this setting to None. An active spare should be present to ensure data integrity in the event of multiple drive failures.
		Queue Full Threshold	Do not change this setting.
		Port ID	This setting should be altered when multiple storage arrays are attached via a switch to ensure that each array is given a unique ID. This is done using the virtual front panel at hardware setup time. This should be performed by an qualified HP technician.
		Port Behavior	Do not change this setting or attached arrays will not be visible to the NAS server.
		Port Topology	Do not change this setting or attached arrays will not be visible to the NAS server.

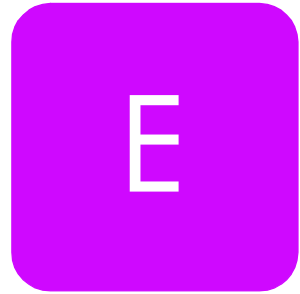
Table 1 Command View SDM Limitations

Tab	Page	Feature	Limitations
Configuration (cont.)	Rebuild	Priority	This is set to Low. If a rebuild is required, you may wish to alter this setting to allow the rebuild to proceed more quickly. This may result in a degradation of user performance.
		Type	Do not changes this setting. Rebuilds are set to automatically occur when required.
		Start/Stop	Disabled unless Manual Rebuild is selected.
Diagnostics	Array	Shutdown	This “turns off” I/O do the array but does not power it down. Doing so without stopping I/O at the NAS server (e.g. turning off all shares/mounts) will cause clients to have I/O failures. Be sure you understand the affects of this operation before using it. The NAS 8000 operating system will automatically start this feature when it boots.
		Full Reset	This feature should not be required in normal operation. Resetting the array can take several minutes. During this time, I/O requests from the NAS server may time out.
		Partial Reset	This feature should not be required in normal operation. This takes less time than a full reset; however, I/O requests from the NAS server may still time out.
		Restart	The inverse of the “Shutdown” operation. It turns back on I/O to the device.
	Disk	Include	This feature is enabled in the Command View NAS web interface.

Table 1 Command View SDM Limitations

Tab	Page	Feature	Limitations
Diagnostics (cont.)		Down	Causes a warning state in the device and a rebuild will be performed if there is an active spare. There may be reasons for doing this, but it should be a rare occurrence.
Download	Array Controller	All	This feature is used to upgrade firmware in the Controller. You can do this without interruption of service.
	LLC Controller	All	This feature is used to upgrade firmware in the Link Level Controller. You can do this without interruption of service.
	Disk	All	<p>This feature is used to upgrade firmware in the drives. You can do this without interruption of service.</p> <p>You must upgrade the firmware on one drive at a time. firmware downloads to drives sometimes fails. This will cause a rebuild which must finish before the next drive can be upgraded.</p>
Performance		All	All of the features on this tab may be freely utilized. The data is not real time data so it has no impact on performance.

Command View NAS Command Line Interface



In addition to the Command View NAS web interface, the HP NAS 8000 also includes a text command interface that allows you to manually enter commands or to run batch commands using either a serial connection or telnet.

The following sections describe the basic functionality of the Command View NAS Command Line Interface. For detailed information on the syntax and parameters for each text command, see the *HP Surestore NAS 8000 Command Reference* on the HP NAS 8000 documentation CD or at the HP support web site (<http://www.hp.com/support/nas8000>).

Logging In

You can log in to the NAS server using a serial connection or telnet.

- 1 Connect to the system:
 - To connect using a serial connection, use a terminal emulator with the following settings:
 - Bits per second: 9600
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None
 - To connect using telnet, enter the following command on a remote computer:
 - telnet xxx.xxx.xxx.xxxwhere xxx.xxx.xxx.xxx is the IP address of the HP NAS 8000 system.

2 Log in to the system.

- Press **Enter** until you see the system name and login prompt.
hp nas8000
NAS OS v1.0.0
localhost login:admin
- Log in as “admin”. No password is required until you set one using the text command interface or the Command View NAS web interface.

Scripting

The HP NAS 8000 command interface is based on Tcl 8.0 (<http://www.scriptics.cXom/software/tcltk/8.0.html>), which allows for powerful scripting commands such as the following:

```
% foreach i [getNetworkCardList] {  
% puts "Network Card Info: $i"  
% puts " ip address = [getNetworkCardIpAddress $i]"  
% puts " subnet mask = [getNetworkCardSubnetMask $i]"  
% }
```

Network Card Info: bond0

```
ip address = 0.0.0.0  
subnet mask = 0.0.0.0
```

Network Card Info: bond1

```
ip address = 0.0.0.0  
subnet mask = 0.0.0.0
```

Network Card Info: eth0

```
ip address = 10.10.0.1  
subnet mask = 255.255.255.0
```


Glossary



A

Access Control List (ACL)	A list associated with a file that contains information about which users or groups have permission to access or modify the file.
Active spare	A previously installed physical drive used as a backup in case an assigned drive fails. The active spare automatically takes over the duties of the failed drive.
Agent	A program that performs a background task for a user and reports to the user when the task is done or some expected event has taken place. The NAS server uses backup agents to back up data remotely.
Aggregation	The combining of multiple similar or related operations into a single one.
Authentication	The process of matching credentials provided by the user against an equivalent entry on the SAM database. A user's name and password are compared against an authorized list and if the system detects a match, access is granted to the extent specified in the permission list for that user.
AutoRAID	AutoRAID implements RAID technology automatically without requiring you to know all the complexities of determining and setting up different RAID modes. AutoRAID is an advanced array storage technology that provides the best combination of cost, performance, and availability.

B

Bond channel	A failover mechanism that automatically switches a specific NIC port to a standby network upon the failure or abnormal termination of the currently active system.
Broadcast address	The address that can be used to send messages to all machines on the subnet. Applying the subnet mask to the IP address provides the subnet.

C

CIFS (Common Internet File System)	A standard way of sharing resources over an IP Network. This standard supercedes SMB.
Cluster	A group of servers that act like a single system.
Collision	The result of two devices transmitting signals at the same time on the same channel, usually resulting in a garbled transmission.
Command View SDM	A web interface for the storage array that lets you manage the storage on the array, monitor the status of the arrays, perform array diagnostics, and download new firmware.
Command View NAS	A web interface for the NAS server that lets you configure, monitor, and upgrade your system as well as manage the storage, contact support, and run diagnostic tools.
Community string	The SNMP keyword required for network management tools to retrieve operational or configuration information from the device.
Credentials	A user's account name and password.

D

Daemon	A program that performs a housekeeping or maintenance utility function without being called by the user. A daemon sits in the background and is activated only when needed, for example, to correct an error from which another program cannot recover.
DHCP (Dynamic Host Configuration Protocol)	Software that automatically assigns IP addresses to client stations logging onto a TCP/IP network. It eliminates having to manually assign IP addresses, and it allows a larger group of machines to share a limited pool of addresses, assuming not all machines are on the network at the same time. DHCP can assign a new address to each machine at startup (dynamic) or permanent (static) addresses can be assigned. Newer DHCP servers dynamically update the DNS servers after making assignments.
Domain (NT)	A group of computers that share a common domain database and security policy.

Domain (TCP/IP)	An alphanumeric representation of an association of computers. (For example, hp.com. com is a top level domain and hp is a second level domain.
Domain Name Service (DNS) Server	A server that translates domain names (such as hp.com) into IP addresses (such as 15.12.255.67). If you have multiple DNS servers on your network, and one DNS server cannot translate a domain name, it asks another one, and so on, until the IP address is found.
Dual In-line Memory Module (DIMM)	A module containing one or several random access memory (RAM) chips on a small circuit board with pins that connect it to the computer motherboard.
E	
Event log	A log of critical or informational events that occurred on the network.
Export	To make a portion of a file system on a remote computer accessible to a local (client) computer.
F	
Failover	A backup operational mode in which the functions of the primary NAS server are assumed by the secondary NAS server when the primary NAS server becomes unavailable through failure or scheduled down time.
Failover package	The smallest unit of failover within the cluster.
File Volume	The basic unit of logical storage for a file system on the NAS server.
G	
Gateway	A combination of hardware and software that links two different networks using different communications protocols so that information can be passed from one to the other. A gateway both transfers information and converts it to a form compatible with the protocols used by the receiving network.
Gateway address	The IP address of a network server or host that functions as a gateway to other networks through communication lines or other network topologies.
GBIC (Gigabit Interface Converter)	A transceiver that converts electric currents (digital highs and lows) to optical signals, and optical signals to digital electric currents. The GBIC is typically employed in fiber optic and Ethernet systems as an interface for high-speed

networking. The data transfer rate is one gigabit per second (1 Gbps) or more.

Group Identification (GID) A number in the UNIX environment that identifies a group of individuals or services to a computer system.

Group quota Lets you restrict the space usage on the NAS server for groups.

H

Heartbeat A periodic signal generated by the server to indicate that it is still running.

High availability High availability characterizes a system that is designed to avoid the loss of service by reducing or managing failures and minimizing downtime. High availability implies a service level in which both planned and unplanned downtime does not exceed a small stated value.

Host Bus Adapter (HBA) An HBA is an I/O adapter that sits between the host computer's bus and the Fibre Channel loop and manages the transfer of information between the two channels. In order to minimize the impact on host processor performance, the host bus adapter performs many low-level interface functions automatically or with minimal processor involvement.

Hot swapping A feature that allows equipment to be connected to an active device, such as a computer, while the device is powered on.

Hub A fibre channel device that connects nodes into a logical loop by using a physical star topology. Hubs will automatically recognize an active node and insert the node into the loop. A node that fails or is powered off is automatically removed from the loop.

I

IP address A unique 32-bit value that identifies network hosts using TCP/IP. An IP address, or block of addresses, is assigned upon application to organizations responsible for that function. No two network hosts can be assigned the same IP address. Each address consists of a network number, optional subnetwork number and host number, written as four numbers separated by periods. Each number can be 0 to 255.

L

LAN (Local Area Network)	A group of computers and other devices, within a specific location (typically within a building or floor of a building), connected by a communications link that enables any device to interact with any other on the network. LANs commonly include microcomputers and shared resources such as laser printers and storage devices.
Logical drive	A logical grouping of one or more physical drives on a system, commonly referred to as a RAID set.
LUN (Logical Unit Number)	A logical unit number (LUN) is a unique identifier used on a SCSI bus that enables it to differentiate between up to eight separate devices (each of which is a logical unit). Each LUN is a unique number that identifies a specific unit of storage, which may be an end user, a file, or an application program.

M

Machine account	All NT workstations and servers on a network must be provided with a machine account in order to participate in a domain.
Media Access Control (MAC) address	A unique, hardware specific address used to identify a network node.
Metadata	Data that describes data. This includes files names, file properties and security information, and lists of block addresses at which each file's data is stored.
Mount	To make a portion of a file system on a remote computer accessible to a local (client) computer. The term is most commonly used with UNIX-based computers.

N

NIC (Network Interface Card)	An expansion card or other device used to connect a computer to a local area network.
NFS (Network File System)	An network protocol designed by Sun Microsystems that allows all network users to access shared files stored on computers of different types. Users can manipulate shared files as if they were stored locally on the user's own hard disk.

With NFS, computers connected to a network operate as clients while accessing remote files, and as servers while providing remote users access to local shared files. The NFS standards are publicly available and widely used.

P

Package control log	A log file is maintained for each package in a cluster. The software and the package monitor log messages that are specific to the package log files. (This feature is available only on high-availability NAS devices.)
Packet	A block of information sent across a network. Packets contain header (which handle addressing), error correction, checksums, and data.
Permission	The ability of a particular user in a multi-user computer environment to access a particular resource by means of a user account. Permissions are stored in the system, in a file called a permissions log. Permissions are checked when a user attempts to access a resource.
Permission bits	Bits that identify the read/write/execute (rwx) privileges for a UNIX file's owner, group, and anyone else that needs access to the file (other).
Physical drive	A term for the hard drives installed in the NAS server. The NAS server can contain up to 12 physical drives.
Primary Domain Controller (PDC)	A server that has been assigned to become the primary authentication server for the Windows NT domain. It stores a copy of the Security Accounts Manager (SAM) database and uses this database to authenticate users.

R

RAID (Redundant Array of Independent Disks)	RAID is a method of combining several disk drives into a single logical storage unit. RAID offers the advantage of fault tolerance by providing real-time data recovery when a disk drive fails, increasing system uptime and network availability. RAID also increases system performance when multiple drives work together.
Redundancy group	Group of physical disks that contain redundant data, as defined by the RAID level assigned to the data. A redundancy group is also divided into logical units (LUNs), addressable by the host. See the <i>HP Surestore Virtual Array VA7100 and VA7400 User And Service Guide</i> for more information on how the VA7100 and VA7400 series differ in their implementation of redundancy groups.

Remote system log A file located on a UNIX machine containing statistics and error messages. See also syslog.

S

SAN (Storage Area Network) Network that connects storage devices and computer systems.

SCSI (Small Computer System Interface) A SCSI interface is used to connect microcomputers to SCSI peripheral devices, such as many hard disks and printers, and to other computers and local area networks.

Security Account Manager (SAM) database A database used to authenticate users.

Share To make files, directories, or folders accessible to other users over a network.

Share level security Share level security for Windows NT is the simplest security method available. Access to file volumes or directories (shares) may be restricted on a share by share basis. The administrator can set read only passwords and read/write passwords for each share on the system. Users wishing to gain access to a share are asked to supply the correct password. Only users with the correct password are given access to the share.

SMB (Server Message Block) protocol A network protocol designed and implemented by Microsoft and used by Windows clients to communicate file access requests to Windows servers. This has been replaced by CIFS.

SMP (Symmetric Multiprocessing) A computer architecture in which multiple processors share the same memory, which contains one copy of the operating system, one copy of any applications that are in use, and one copy of the data. Because the operating system divides the workload into tasks and assigns those tasks to whatever processors are free, SMP can potentially service more transactions within a fixed amount of time than a single processor system.

SMTP (Simple Mail Transfer Protocol) A TCP/IP protocol for sending messages from one computer to another on a network. This protocol is used on the internet to route email.

SNMP (Simple Network Management Protocol) The network management protocol for TCP/IP. In SNMP, agents, which can be hardware as well as software, monitor the activity in the various devices on the network.

Snapshot	A read-only copy of a file volume that contains an image of the volume as it appeared at the point in time when the copy was taken.
Subnet Mask	A 32-bit numeric mask that blocks out all but the necessary information. This allows the IP address to be broken into a component that identifies the subnet on which the device resides and the ID of the device itself.
Switch	A device that provides a crossbar connection so any one port may be connected to any other port at any one instant such that multiple connections are occurring.
Syslog	The main system log that contains statistics and error messages. This log resides in <code>/var/log/messages</code> .
System log	A file containing statistical information and error messages.
System name	The system name uniquely identifies your NAS server. It is a text string up to 15 characters drawn from the alphabet (A-Z), digits (0-9), and minus sign (-). Note that periods are only allowed when they serve to delimit components of "domain style names." No blank or space characters are permitted as part of a name. No distinction is made between upper and lower case. However, the name must begin with a letter and the last character must not be a minus sign. The name you use appears on the Identity screen of the user interface and in Network Neighborhood in a Windows networking environment.

T

TCP/IP	A commonly used networking protocol that allows interconnection of different network operating systems. TCP/IP stands for Transmission Control Protocol/Internet Protocol.
Telnet	A protocol that provides console services remotely. The Telnet program runs on your computer and connects your PC to the NAS server through the network. You can enter commands through the Telnet program and they are executed as if you were entering them directly on the server console.
Trap	A type of SNMP message used to signal that an event has occurred.

U

UPS (Uninterruptible Power Source)	A device that is connected between a computer (or other electronic equipment) and a power source that ensures that electrical flow to the
---	---

computer is not interrupted because of a blackout. UPS protects the computer against potentially damaging events such as power surges and brown-outs.

User authentication

See Authentication.

User Identification (UID)

A unique number in the UNIX environment that identifies an individual to a computer system.

User level security

The NAS server uses a domain controller to authenticate users when they access the device. Access Control Lists (ACLs) define a user's access rights to a particular object. Users accessing the resources of the system must be logged onto an NT domain and must have specific rights to access the given resource. The resource is not only the share, but the directories and files within the share as well. Administrators and users may restrict access to any file, directory, or group of files and directories to any user or group of users in the domain.

User quota

Lets you restrict the space usage on the NAS server for users.

V**Volume group**

An aggregation of one or more LUNs.

W**WINS (Windows Internet Naming Service)**

The Windows NT Server method for associating a computer's hostname with its address.

Workgroup

A group of computers on a network that connect to each other using peer relationships.

index

A

- active/active failover model **24**
- active/passive failover model **24**
- adding disks **187**
- alerts settings **43**
 - SMTP/email **71**
 - SNMP **70**
 - Syslog **72**
- anti-virus software **128**
- architecture **13**
- ARCserve 2000 **165**
- array **10**
 - firmware **181**
 - renaming **79**
 - scanning for **79**
 - upgrade **187**
- asset number **52**

B

- backup agent **140**
 - HP OpenView OmniBack II **141**
- backup applications supported **159**
- Backup Exec **167**
- bonding, enabling **56**

C

- client activity **124**
- cluster **24**
 - configuration **59, 61, 62, 63, 64**
- command line interface **221**
- Command View NAS **35**
- Command View SDM **213**

- advanced array management **80**
- Computer Associates ARCserve 2000 **165**
- configuration tab **43**
 - administrative password **49**
 - date and time **52**
 - DNS **58**
 - informational settings **52**
 - NFS properties **69**
 - NIS properties **68**
 - remote system log **72**
 - SMTP/email **71**
 - SNMP **70**
 - system name **51**
 - TCP/IP **54**
 - UPS settings **76**
 - user and group mapping **73**
 - Windows security **66**
 - WINS properties **66**
 - wizard **44**
- Configuration Wizard **44**
- configuring the cluster **59, 61, 62, 63, 64**
- configuring the NAS server **19**
- contact information **52**
- cooling fans **120**
- CPU utilization **123**
- creating
 - directory **98**
 - exports **96**
 - file volume **92**
 - LUN **80**
 - shares **96**
 - snapshots **101**
- customer support **176**

- phone 176
- requesting information 176
- URL 176

D

- date settings 52
- deleting
 - directory 99
 - file volume 94
 - LUNs 81
 - snapshots 102
- DHCP 54
- diagnostic tools 179
- directories 21
 - creating 98
 - deleting 99
 - renaming 99
- disabling software 127
- disaster recovery 153
- disk drive configuration 21
- DNS 58
- Domain Name Service 58
- Dynamic Host Configuration Protocol (DHCP) 54

E

- email notification of hardware failure 71
- enabling
 - bonding 56
 - software 127
- error notification
 - email 71
 - SNMP server 70
- event log 118
- exports 95
 - creating or editing 97
 - deleting 97

F

- failover models 24
- failover packages 24
 - adding 86

- deleting 88
- editing 87
- manual failback 90
- manual failover 89
- monitoring 125
- starting 88
- stopping 89
- viewing 85
- file volumes 21
 - creating 92
 - deleting 94
 - editing 93
 - renaming 93
 - viewing information 95

G

- getting started 19
- group mapping 73
- group quota 109
 - adding 110
 - deleting 111
 - editing 110
 - enabling/disabling 105
 - importing/exporting 111

H

- hardware event log 117
- hardware overview 10
- heterogeneous environment security 32
- high availability 24
 - direct-attached configuration 13
 - SAN configuration 13
 - upgrading to 183
 - virus protection 128
- host allow list 96
- HP authorized resellers 184
- HP limited warranty statement 211
- HP OpenView OmniBack II 161
- HP Virus Guard 128

I

IBM Tivoli Storage Manager 171
identity tab 46
importing and exporting users or groups 75
informational settings 52
installation 19
IP addresses 54

J

Java plug-in 35

L

Legato NetWorker 173
log file of NAS server events 118
LUN 21
 creating 80
 deleting 81
 managing 80

M

management port 56
mapping NT and UNIX users or groups 73
memory status 121
mixed-mode security 32
monitor hardware status 115

N

NAS 9
NAS server 10
 Command View NAS web interface 35
 configuration options 13
 restarting 47
 shutting down 47
 software 10
 software upgrade 180
 upgrade 184
NetBackup 169
network activity 123
network attached storage (NAS) 10
network backup applications 159
 ARCserve 2000 165

Backup Exec 167
NetBackup 169
NetWorker 173
OmniBack II 161
 Storage Manager 171
Network Card Parameters 54
Network File System 69
Network Information Services 68
network settings 43
 DNS 58
 NFS 69
 NIS 68
 TCP/IP 54
 Windows security 66
 WINS addresses 66
network time protocol 52
NetWorker 173
NFS export 97
NFS properties 69
NIC ports 54
NIS properties 68
NTP 52

O

OmniBack II 161
online help 39
 printing 39
Open Source 178

P

package control log 113
partition a drive 92
password changing or removing 49
password file management 49
physical storage 21
port
 management 56
 NIC 54
power supply status 121
printing help files 39
product configurations 13

- purchasing
 - hardware and upgrades **184**
 - software upgrades **180**

Q

- quotas **105**

R

- racked system **10**
- real time protection **135**
- regulatory compliance information **208**
- remote system log **72**
- resource model **24**
- restarting the NAS server **47**
- RTP **135**

S

- SAN configuration **13**
 - shutting down **47**
 - with high availability **13**
- scheduled scan control **131**
- security **29**
 - mixed mode **32**
 - Windows NT **30**
- shares **95**
 - creating or editing **96**
 - deleting **97**
- shutting down or restarting **47**
 - direct-attached configuration **47**
 - high-availability configuration **47**
 - SAN configuration **47**
- Simple Mail Transfer Protocol **71**
- Simple Network Management Protocol **70**
- single points of failure **24**
- SMB share **96**
- SMTP **71**
- snapshots **21**
 - creating **101**
 - deleting **102**
 - editing **102**
 - enabling **152**

- renaming **102**
- scheduling **103**
- using **100**

- SNMP **70**

- software license agreement **203**
- software upgrade **180**
- status summary **115**
- status tab **113**
- storage
 - overview **21**
- storage array **10**
 - diagnostics **179**
 - firmware **181**
 - upgrade **187**
- storage array summary **78**
- Storage Manager **171**
- storage tab **77**
- support **176**
- support tab **175**
- syslog **72**
- system log **118**
- system messages **118**
- system name **51**
- system settings **43**
 - administrative password **49**
 - date and time **52**
 - informational **52**
 - system name **51**
- system voltage **119**

T

- tape devices **141**
- tape library **10**
 - upgrade **190**
- TCP/IP settings **54**
- telnet **221**
- temperature **119**
- text command interface **221**
- time settings **52**
- Tivoli Storage Manager **171**
- trap definitions **197**

U

upgrade

- high availability **183**
- purchasing hardware **184**
- server **184**
- software **180**
- storage array **187**
- storage array firmware **181**
- tape library **190**
- UPS **195**

UPS

- connections **76**
- status **122**
- upgrade **195**

user mapping

user quota

- adding **107**
- deleting **108**
- editing **107**
- enabling/disabling **105**
- import/export **108**

using help

V

Veritas

- Backup Exec **167**
- NetBackup **169**

viewing

- client activity **124**
- cooling fans **120**
- CPU utilization **123**
- file volume information **91**
- hardware event log **117**
- memory status **121**
- network activity **123**
- power supply status **121**
- system log **118**
- system voltage **119**
- temperature **119**
- volume groups **82**

virtual IP address

Virus Guard

virus protection

virus protection for high-availability NAS server

voltage status

volume group

- creating **82**
- deleting **84**
- editing **83**
- overview **21**
- renaming **83**

W

web interface

Windows

- creating shares **96**
- properties **66**
- security **66**

Windows NT security configuration

WINS addresses

WINS servers

X

XP

